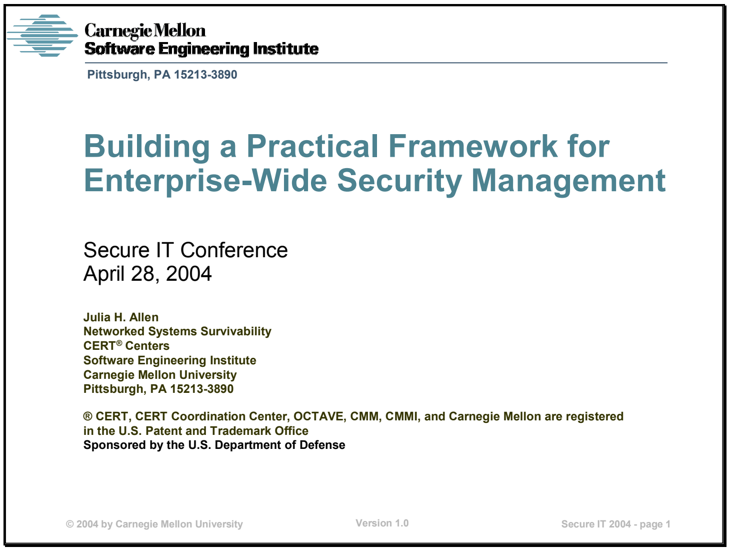
Slide 1



Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

Building a Practical Framework for Enterprise-Wide Security Management

Secure IT Conference
April 28, 2004

Julia H. Allen
Networked Systems Survivability
CERT® Centers
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

® CERT, CERT Coordination Center, OCTAVE, CMM, CMMI, and Carnegie Mellon are registered in the U.S. Patent and Trademark Office
Sponsored by the U.S. Department of Defense

Carnegie Mellon University's Software Engineering Institute's CERT® Centers are working with executives in commercial and government organizations to develop a practical framework for enterprise-wide security management. They have found that current efforts to manage security vulnerabilities and security risks only take an enterprise so far, with results degrading over time and as complexity increases. What is needed is a framework that (1) mobilizes key enterprise functions to achieve and sustain a desired security state in the normal course of business and (2) addresses the proliferation of security regulations, standards, checklists, scorecards, assessments, and audits. This presentation describes work in progress on such a framework.

The author acknowledges the contribution of the following individuals to the content of this presentation:
Kevin Behr, IP Services and ITPI
Rich Caralli, SEI
Eileen Forrester, SEI
Gene Kim, Tripwire and ITPI
Larry Rogers, SEI
Jeannine Siviy, SEI
Bill Wilson, SEI

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **28 APR 2004**	2. REPORT TYPE	3. DATES COVERED **00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE **Building a Practical Framework for Enterprise-Wide Security Management**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
presented at the Secure IT Conference, 27-30 April 2004, San Francisco, CA.

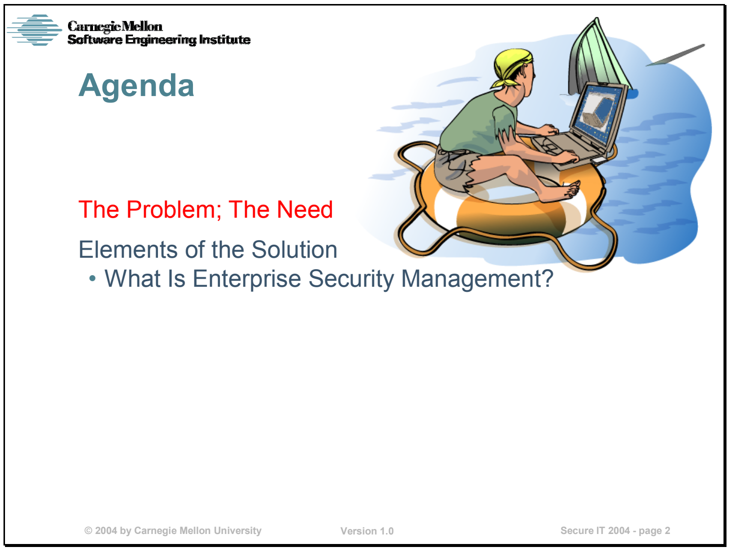
14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**58**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Slide 2



Carnegie Mellon
Software Engineering Institute

Agenda

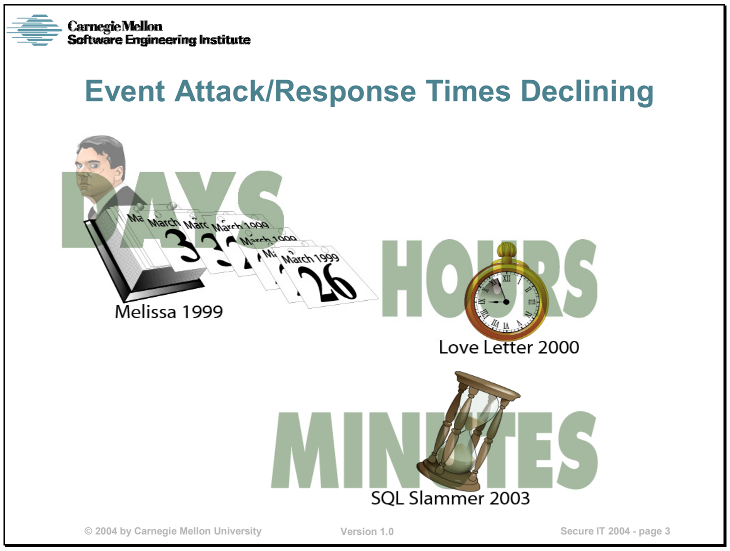
The Problem; The Need

Elements of the Solution
- What Is Enterprise Security Management?

Version 1.0

This presentation first describes the problem from a reactive/intruder-based perspective, as we in the security community typically consider it. What becomes clear is that we cannot continue to attempt to solve the ‘security problem’ solely from this point of view. We will never catch up or be able to fully anticipate new and increasingly sophisticated attack patterns – or even old ones with known solutions that continue to proliferate. We must begin to broaden the solution to encompass an enterprise wide, proactive, and controls- and process-based approach that addresses impact, not just threat and vulnerability. From this broader vantage point, we offer several promising ways to think about the problem and tackle it effectively, based on current work with high performing organizations. We call this approach Enterprise Security Management.

Slide 3



Carnegie Mellon
Software Engineering Institute

Event Attack/Response Times Declining

DAYS

Melissa 1999

HOURS

Love Letter 2000

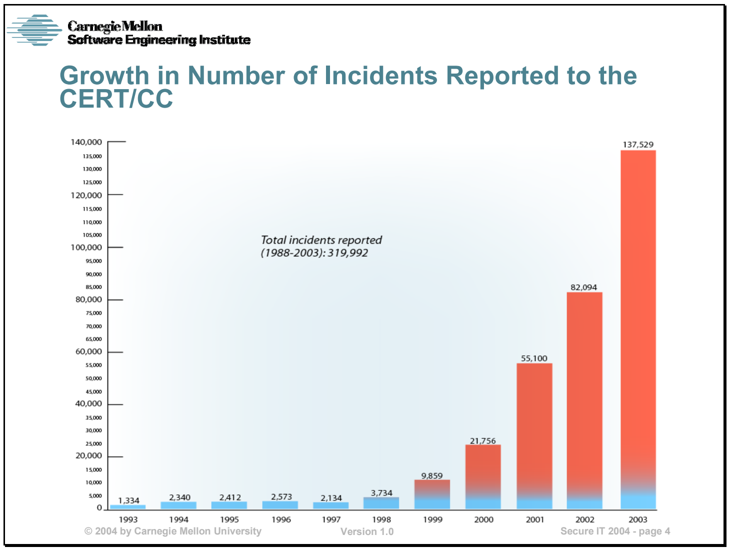
MINUTES

SQL Slammer 2003

Version 1.0

The amount of time for new attacks to emerge and affect a significant number of Internet-connected networks and hosts has been declining by orders of magnitude over the last several years. Melissa, which occurred in March 1999, took days to spread; Love Letter, which first appeared in May 2000, took hours as did Code Red (July 2001) and Nimda (September 2001). Slammer, which first appeared in January 2003, took only minutes as did Blaster/SoBig (August 2003). In addition, Slammer capitalized on a vulnerability six months after the vulnerability was announced; Blaster/SoBig appeared only 26 days after their companion vulnerabilities were announced.

Slide 4



Carnegie Mellon
Software Engineering Institute

Growth in Number of Incidents Reported to the CERT/CC

© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 4

An incident is defined as any real or suspected adverse event in relation to the security of computer systems or networks and also as the act of violating an explicit or implied security policy.

Examples include:

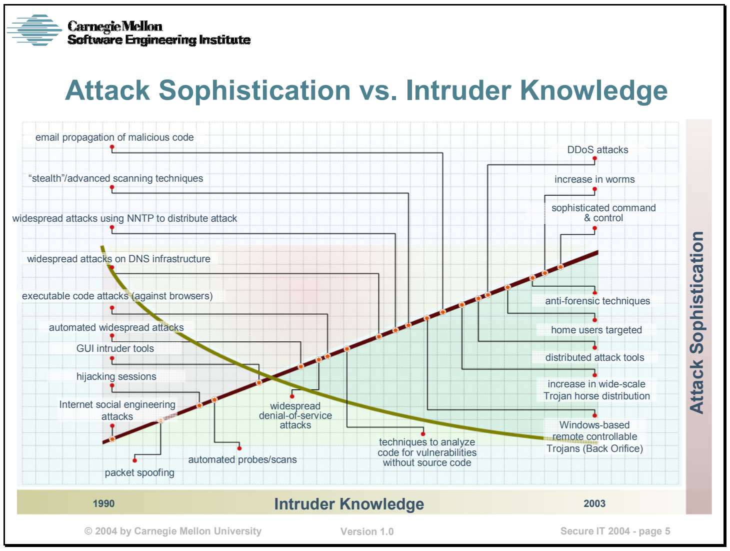
failed or successful attempts to gain unauthorized access to a system or its data
unwanted disruption or denial of service
the unauthorized use of a system for the processing or storage of data
changes to systems without the owner's consent
the occurrence of computer viruses
probes (single attempt) or scans (multiple attempts) of a range of computer systems via the network, seeking vulnerabilities

For example, CERT classifies Melissa, Code Red, and Blaster each as a single incident, which makes the above trend even more alarming.

The number of incidents reported to CERT/CC went up 164% in 1999, 121% in 2000, 153% in 200, 49% in 2002, and 68% in 2003.

This growth can be attributed to a number of factors including more computers attached to the Internet, more information assets at stake (and therefore worthy of attack), more people reporting incidents (likely to a wide range of response centers in addition to CERT), CERT becoming better known as a safe haven for incident reporting, and, of course, an increase in the number of incidents. At this time, we have not analyzed reports to determine the cause of the increase.

Slide 5



Carnegie Mellon
Software Engineering Institute

Attack Sophistication vs. Intruder Knowledge

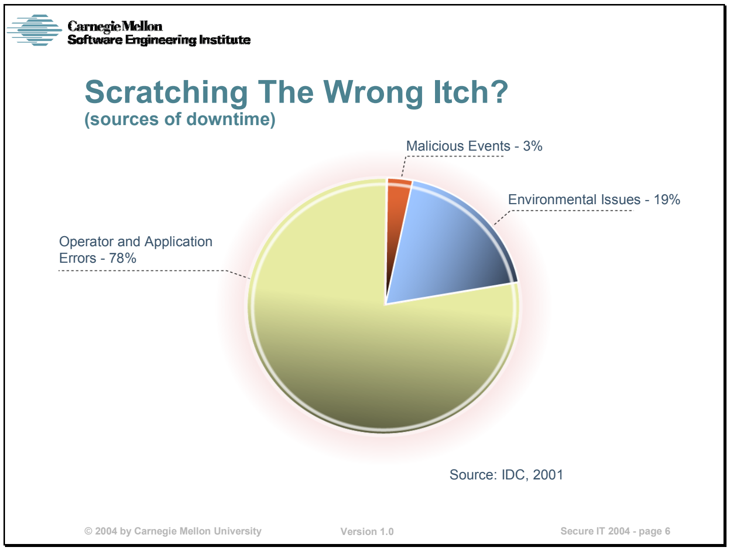
© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 5

Trends indicate that the sophistication of attack tools is increasing while the amount of individual technical knowledge required to launch an attack is decreasing. Attack knowledge is either in the skills of an individual or captured in a software tool that can be widely shared. It takes less than 2 minutes for an unsophisticated attacker to download an automated tool from the Internet and attack a site.

[More detail: In the 1980s intruders were the system experts. They had a high level of expertise and personally constructed the methods for breaking into systems. Using automated tools and exploit scripts was the exception rather than the rule. Today, absolutely anyone can attack a network. This is due to the widespread and easy availability of intrusion tools and exploit scripts that can easily duplicate known methods of attack. While experienced intruders are getting smarter, as demonstrated by the increased sophistication in the types of attacks, the knowledge required on the part of novice intruders to copy and launch known methods of attack is decreasing. Meanwhile, as evidenced by distributed denial-of-service attacks and variants of recent viruses and worms, the severity and scope of attack methods is increasing.

In the early/mid 1980s, intruders manually entering commands on their personal computer could access tens to hundreds of systems; today, intruders use automated tools to access thousands to tens of thousands of systems. In 1980s, it was relatively straightforward to determine if an intruder had penetrated your systems and discover what they did. Today, intruders are able to totally hide their presence by, for example, disabling commonly used services and reinstalling their own versions, and erasing their tracks in audit and log files. In the 1980s and early 1990s, denial-of-service attacks were infrequent and not considered serious.Today, for organizations such as Internet service providers that conduct business electronically, a successful denial-of-service attack can put them out of business. Unfortunately, these types of attacks occur more frequently each year.]

Slide 6


Carnegie Mellon
Software Engineering Institute

Scratching The Wrong Itch?

(sources of downtime)

Source: IDC, 2001

© 2004 by Carnegie Mellon University

Version 1.0

Secure IT 2004 - page 6

According to IDC, only 3% of network and system down time (lack of availability) stems from malicious events (launched from inside or outside of an organization's networks). In part, this could be because, as a community, we have focused heavily on protecting networks from these events and have become more effective at keeping them from causing outages. But what about the remaining 97%?

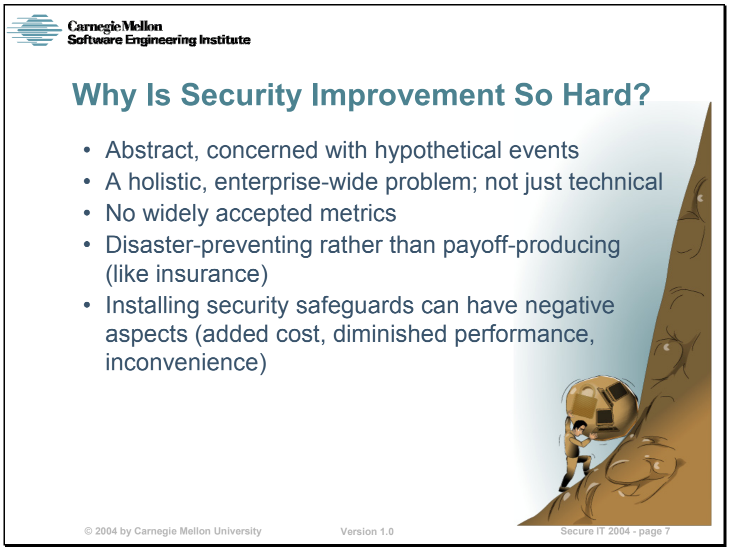
19% result from environmental issues, such as power outages, fiber cuts, etc. – primarily physical events.

The majority – 78% – comes from operator and application errors. These range from people copying files to the wrong place, accidentally deleting files, or making changes that cause problems in the operation of systems.

Major security breaches (defined by a CompTIA survey as those that caused real harm, resulting in the loss/disclosure of confidential information or interrupted business) are slowly increasing and are most often attributed to human error (47%), rather than technical problems. CompTIA found that 80% of respondents attribute the breaches to a lack of IT security knowledge, a lack of training, or a failure to follow security procedures. Nearly 1 in 5 of those surveyed reported that none of their IT staff have any formal security training. [A survey of 896 Computing Technology Industry Association (CompTIA) members and IT security professionals last December]

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci958579,00.html?track=NL-102&ad=479694

When it comes to system availability and reliability, addressing security issues alone will not solve the problem.



Carnegie Mellon
Software Engineering Institute

Why Is Security Improvement So Hard?

- Abstract, concerned with hypothetical events
- A holistic, enterprise-wide problem; not just technical
- No widely accepted metrics
- Disaster-preventing rather than payoff-producing (like insurance)
- Installing security safeguards can have negative aspects (added cost, diminished performance, inconvenience)

Version 1.0

Why is security improvement so hard to sell? So hard to implement?

Security, for most, is abstract, concerned with hypothetical events

Security is a holistic, not just a technical, problem; technological, organizational, regulatory, economic, and social aspects interact

There are no widely accepted metrics for characterizing security or (de facto) standards of best practice

The Internet's cyber security state today is far worse than what known best practices can provide. This is particularly alarming for national critical infrastructures such as communication, transportation, financial transaction processing, and utilities (power, gas, water) distribution.

Security measures are typically viewed as disaster-preventing rather than payoff-producing (like insurance), which makes it difficult to justify investing in security.

Benefits can be seen only in events that do not happen (impossible to prove a negative, valuing cost avoidance). This same difficulty has stalked efforts to improve software quality, conduct proper testing, keep documentation up-to-date, maintain current configuration and hardware/software inventory records, etc. [Braithwaite]

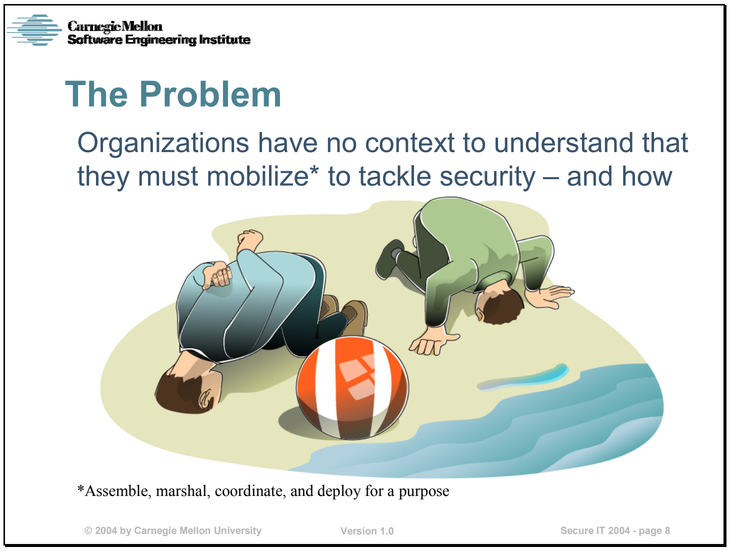
Installing security safeguards has negative aspects (added cost, diminished performance, inconvenience, etc.)

"Cybersecurity Today and Tomorrow: Pay Now or Pay Later," Computer Science and Telecommunications Board, National Research Council. National Academy Press, Washington, DC. Prepublication edition. http://books.nap.edu/html/cybersecurity/

With respect to the last two bullets above: "The principal accusation was that Y2K was a relatively minor problem that had been created by consultants to obtain work and that the whole thing had been greatly over-hyped. Accusers held that the accusation was true simply because nothing much happened at the rollover. It is important to acknowledge this type of thinking because of the distinct possibility that architects of a successful cyber security program may find themselves under attacks similar to those leveled at the solvers of Y2K." Timothy Braithwaite. "Executives Need to Know: The Arguments to Include in a Benefits Justification for Increased Cyber Security Spending." *Information Systems Security*, Auerbach Publications, September/October 2001.

See also Schneier, Bruce. "Hacking the Business Climate for Network Security." Computer, IEEE, April 2004.

Slide 8



Carnegie Mellon
Software Engineering Institute

The Problem

Organizations have no context to understand that they must mobilize* to tackle security – and how

*Assemble, marshal, coordinate, and deploy for a purpose

Version 1.0

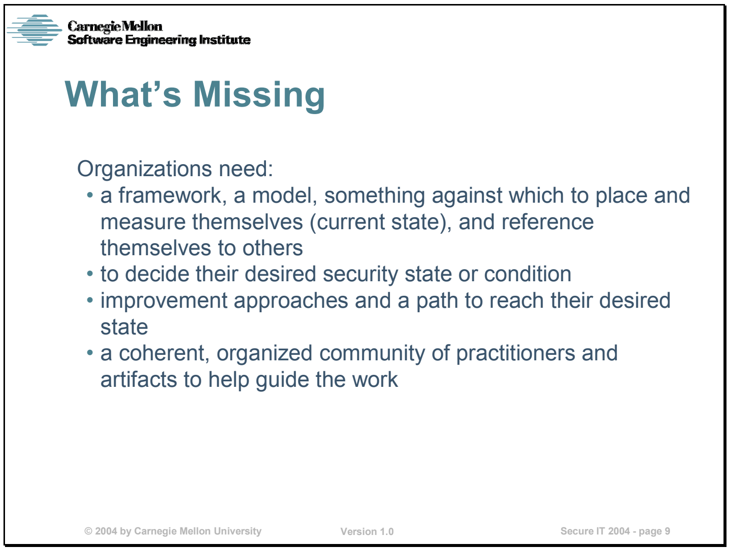
Security lives in an organizational and operational context, not as a standalone discipline. This context has not been well defined from a security perspective. It includes all of an organization's capabilities that need to be brought to bear, to mobilize if you will, to make security happen, both to achieve a secure state and to sustain it – and what "it" means.

The idea is to take what an organization is already doing well and apply these capabilities to managing security at an enterprise level, thus taking actions that are no different (conceptually) from those needed to meet any other requirement of conducting business. Examples of such capabilities include risk management, project management, and audit.

Once we describe this context, we can define in more detail the capabilities that we believe are most promising in making a contribution to security and a suggested order to tackle them (or at least of series of decision aids to aid in determining this). For example, can internal audit be used as an enabler to bring about an accelerating effect to improve security? And if you find out in implementing your security improvement that it is not about security at all but about executing a well-defined IT operational process (such as change management) within which you embed security controls, then what role does process improvement play in helping you articulate, define, document and improve your IT processes?

We know from other domains (like software development) that a focus on organizational and operational issues gives an organization a range of direct and indirect business advantages. It's possible that effective security will simply be among the desirable outcomes of a focus on the right operational and organizational issues. We discuss this further in describing our work with high-performing organizations.

Slide 9



Carnegie Mellon
Software Engineering Institute

What's Missing

Organizations need:

- a framework, a model, something against which to place and measure themselves (current state), and reference themselves to others
- to decide their desired security state or condition
- improvement approaches and a path to reach their desired state
- a coherent, organized community of practitioners and artifacts to help guide the work

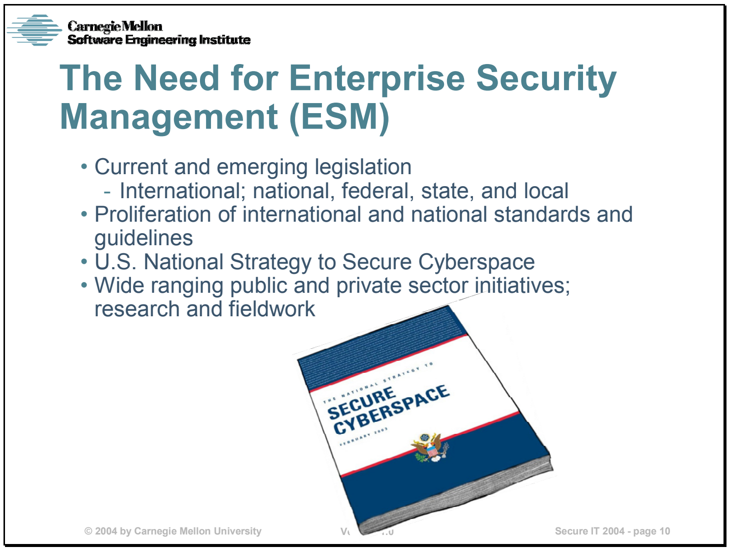
Version 1.0 Secure IT 2004 - page 9

To achieve and sustain a desired security state, organizations need a framework – some type of roadmap or yardstick to determine where they are and in reference to their peers. This framework needs to tie to business objectives.

Such a framework also describes a set of behaviors, processes, and practices that articulate a high performing security state (with respect to at least the fundamental security requirements of confidentiality, availability, and integrity). Using business objectives as the selection criteria, organizations can then determine how far along the spectrum from current to high performing they need to be.

To move from a current state to a desired state using a framework requires a range of implementation approaches and decision aids. Certainly last, but not least, an improvement program must be informed by fellow travelers who have passed this way before, from whom to learn and whose work can be codified to serve as useful guidelines on what to do, why to do it, and how to measure progress along with costs vs. benefits.

Slide 10



Carnegie Mellon
Software Engineering Institute

The Need for Enterprise Security Management (ESM)

- Current and emerging legislation
  - International; national, federal, state, and local
- Proliferation of international and national standards and guidelines
- U.S. National Strategy to Secure Cyberspace
- Wide ranging public and private sector initiatives; research and fieldwork

© 2004 by Carnegie Mellon University

Secure IT 2004 - page 10

There is a wide range of current and pending legislation that calls for improvement in how we manage our organizational infrastructures and the information they create, transmit, and store. These include the Family Educational Rights Privacy Amendment (FERPA) for educational institutions, Federal Information Systems Management Act for federal agencies, Health Insurance Portability and Accountability Act (HIPAA) for those in health care, Gramm-Leach-Bliley Act for financial institutions, Sarbanes-Oxley for publicly traded institutions, Child Online Privacy Protection Act (COPPA), Basel II Capital Accord for international financial institutions, and California's Database Security Breach Notification Act (SB 1386) for consumer privacy.

There are an ever growing number of standards, guidelines, checklists, and assessment instruments with which organizations are expected to demonstrate some level of compliance (refer to the slides titled Framework Sources).

Certainly the US federal government has recognized the potential impacts of breaches in security on critical infrastructures in its National Strategy to Secure Cyberspace, published in 2003, which contains a wide range of recommendations calling for improvement. Most recently, the National Cyber Security Partnership has announced the release of public/private sector task force reports containing recommendations for improving home user and small business awareness, early warning, security in the software development life cycle, information security governance, and technical standards (refer to http://www.cyberpartnership.org/).

At the SEI, we see this need reinforced in the following areas of work:

Material on security is in high demand as new content in the CMMI® (Capability Maturity Model Integration) model

Experience of the CERT Centers (http://www.cert.org)

Development, piloting, and transition of OCTAVE (http://www.cert.org/octave)

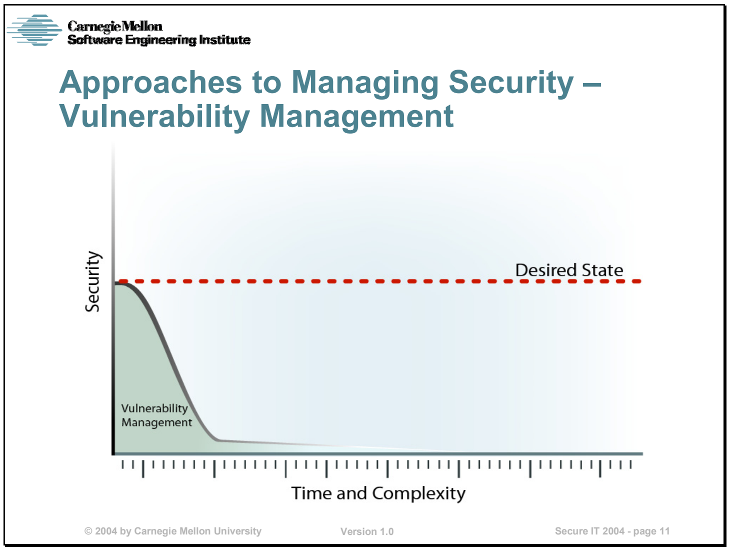
Work with organizations to define security needs and link them explicitly to business drivers using methods such as Critical Success Factors and Six Sigma

Work with high performing organizations who are achieving security goals through operational excellence

Demands for various forms of executive outreach and education in information security

Experience in Computer Security Incident Response Team (CSIRT) development and deployment (http://www.cert.org/csirts)

Slide 11



Carnegie Mellon
Software Engineering Institute

Approaches to Managing Security – Vulnerability Management

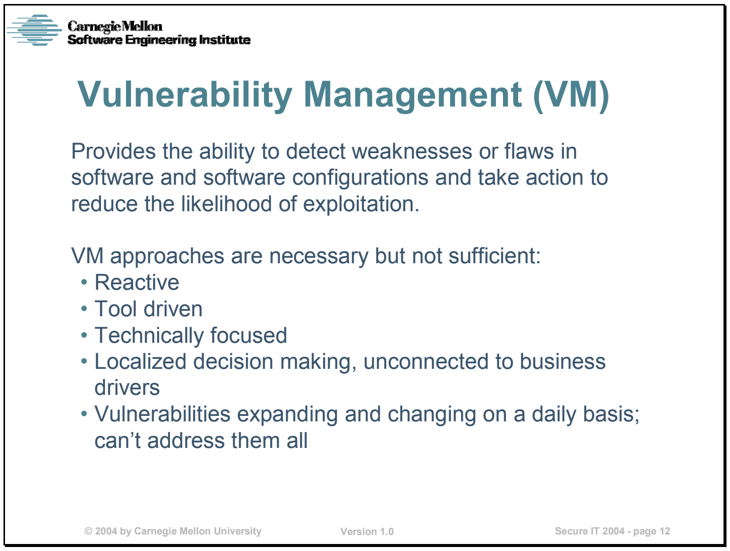
Security
Desired State
Vulnerability Management
Time and Complexity

© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 11

An organization's first attempt to address security is likely ad hoc incident response, such as dealing with a virus infestation. Once an organization gets bitten by more of these than they care to mention and realizes that there are some known solutions (such as closing vulnerabilities) to help reduce the pain, they move to vulnerability management (VM). VM provides the ability to detect weaknesses or flaws in software and software configurations and take action to reduce the likelihood of exploitation.

Active management of vulnerabilities is an improvement over the less mature incident response practice. Small or less complex organizations may find that vulnerability management is sufficient to sustain their desired security state. (It does not matter for this discussion what the desired state is, and it is often the case that the desired state shifts as conditions and the environment change.) However, as time and organizational complexity increase (including broader connectivity with vendors, partners, and collaborators), the ability of VM to sustain a desired security state diminishes.

Slide 12



Carnegie Mellon
Software Engineering Institute

Vulnerability Management (VM)

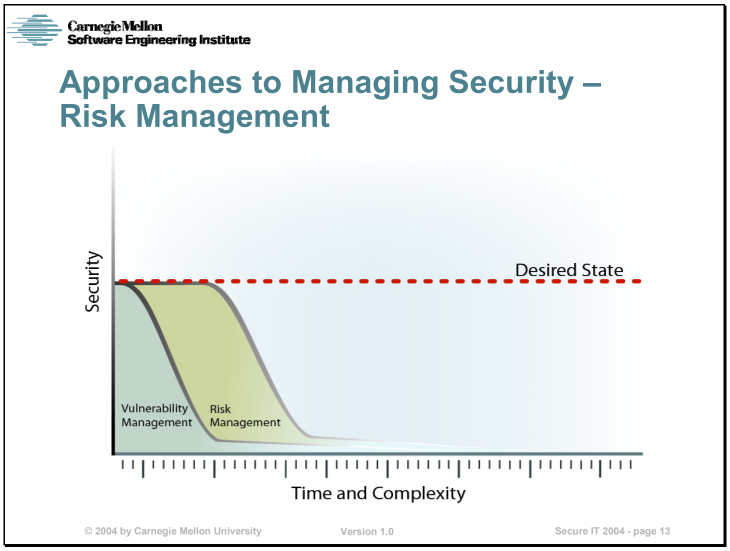
Provides the ability to detect weaknesses or flaws in software and software configurations and take action to reduce the likelihood of exploitation.

VM approaches are necessary but not sufficient:

- Reactive
- Tool driven
- Technically focused
- Localized decision making, unconnected to business drivers
- Vulnerabilities expanding and changing on a daily basis; can’t address them all

Vulnerability management is necessary but not sufficient; in other words, for most organizations, it’s part of the solution but not the entire solution. VM tends to be reactive, tool driven, focused on technology, performed primarily by technicians, with too little connection to business drivers and mission, and focused on information or network security, leaving out other organizational issues. Vulnerabilities are expanding and changing on a daily basis; organizations cannot keep up.

Slide 13



Carnegie Mellon
Software Engineering Institute

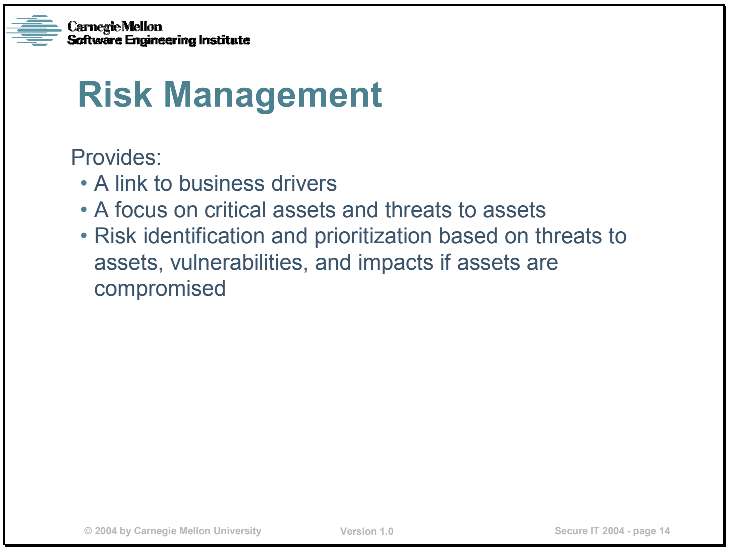
Approaches to Managing Security – Risk Management

Version 1.0 Secure IT 2004 - page 13

We have advocated risk management for several years to improve security (http://www.cert.org/octave). We do find that an effective security risk-management approach allows an organization to sustain their desired security state more reliably and over time than solely an ad hoc incident response or vulnerability management approach. This is because effective security risk management focuses on the security of key assets that are critical to meeting the mission (as contrasted with all assets). Identified and prioritized risks aid in determining the most effective security actions to take. Risk-mitigation activities also tend to be selected and executed with organizational business drivers in mind.

However, the effectiveness and ability of risk management to sustain a desired security state also falls off as time and organizational complexity increase. In part, this is because the security risk management approach does not sufficiently account for all the enterprise issues.

Slide 14



Carnegie Mellon
Software Engineering Institute

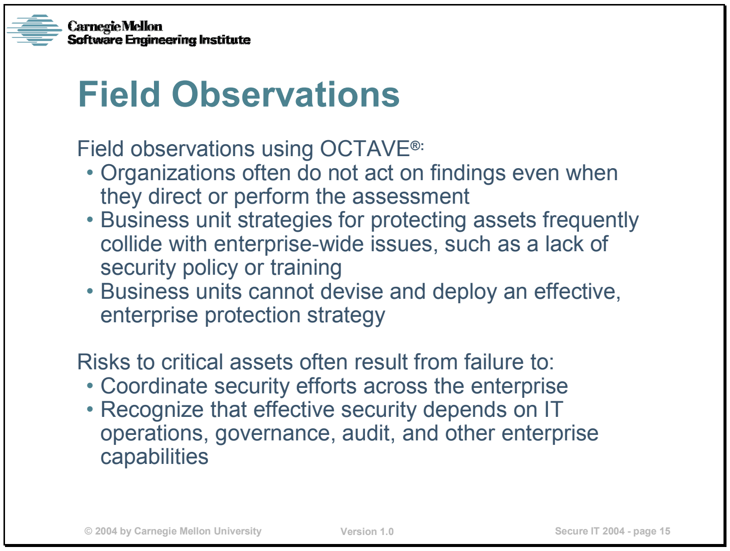
Risk Management

Provides:

- A link to business drivers
- A focus on critical assets and threats to assets
- Risk identification and prioritization based on threats to assets, vulnerabilities, and impacts if assets are compromised

Version 1.0 Secure IT 2004 - page 14

Information security risk management, particularly when considered in concert with other organizational risk management processes, does provide a connection to business objectives and drivers. Most approaches address the identification of enterprise security requirements, the assets that play the biggest role in meeting these requirements and their criticality (impact to the organization if the asset is lost, compromised, destroyed, revealed), potential threats to such assets, vulnerabilities that can be used to realize these threats, and the requisite impacts. Once this information is well understood, organizations can prioritize risks, define action plans, and determine levels of appropriate investment.



Carnegie Mellon
Software Engineering Institute

Field Observations

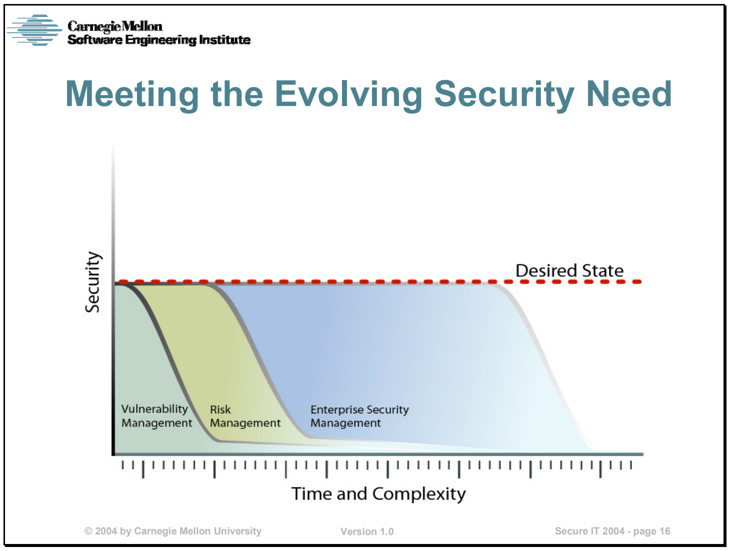
Field observations using OCTAVE®:
- Organizations often do not act on findings even when they direct or perform the assessment
- Business unit strategies for protecting assets frequently collide with enterprise-wide issues, such as a lack of security policy or training
- Business units cannot devise and deploy an effective, enterprise protection strategy

Risks to critical assets often result from failure to:
- Coordinate security efforts across the enterprise
- Recognize that effective security depends on IT operations, governance, audit, and other enterprise capabilities

Field work in using the OCTAVE method has shown that even when an organization takes charge of the information security risk evaluation, it is no more likely to act on the findings of the evaluation. This typically occurs because the evaluation is performed at an operational, business unit level where localized decisions can be made, but there are significant barriers to extrapolating those decisions to an enterprise level, where they can benefit the entire organization and enable successful improvement at the local level.

While the OCTAVE method provides for the development of a protection strategy for the enterprise, it is actually rooted in the operational unit's perception of the enterprise. If the organization has no framework in which to accept these localized findings and strategies and mobilize them to benefit the entire organization, localized efforts become stalled, and organizational learning is diminished. As this cycle continues, the organization has less control over maximizing the protection of critical assets through their security efforts.

Slide 16


Carnegie Mellon
Software Engineering Institute

Meeting the Evolving Security Need

© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 16

This figure illustrates some of our current understanding of an approach such as ESM. We have recognized that vulnerability management and security risk management alone do not allow organizations to reach and sustain their desired security state for very long. These approaches may work when the organization isn't organizationally or technically complex, but as complexity increases, the efficacy of vulnerability and security risk management to sustain the desired state falls off.

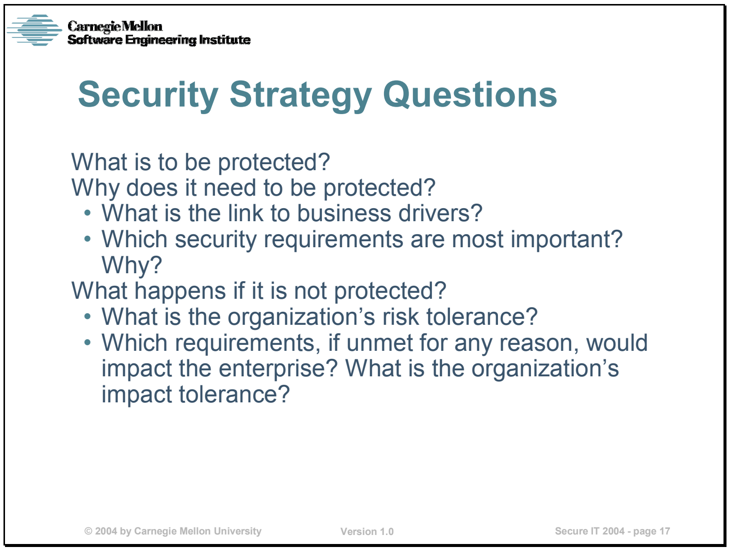
We assert that an enterprise security management approach will allow the organization to achieve and maintain a desired state because all of the organizational and operational processes and participants relevant to security are engaged.

We are considering whether there may be another condition beyond the ESM area depicted above, which we characterize as "transparency" or "resiliency." We see a trace of this in some literature and in some discussions with high performers. The idea is that extremely capable organizations may no longer need to focus specifically on security. Their operational excellence produces appropriate security as a side effect. In fact, some high performing organizations object to our focus on security—their goal is operational excellence and security appropriate to their business drivers is simply one of their operational requirements.

So the range of potential approaches we observe (or posit in the case of transparency) are ad hoc incident response, active vulnerability management, security risk management, possibly an intermediate step of deploying security controls as part of mature IT operational processes, enterprise security management, and transparency. It is possible to conceive of these as characterizations of increasing maturity, but we will not know until we do further work if that characterization is necessary or accurate. It may be better to conceive of these as a range of appropriate security approaches depending on the complexity of the enterprise. In brief, it seems safe to say that capability to manage security throughout the enterprise must increase as complexity and time increase if the organization wants to achieve and sustain its desired security state.

In short, using vulnerability management, an organization has some modest level of protection but is unable to define and act to implement a desired security state. Using risk management, an organization is capable of defining a desired state, but will have great difficulty in attaining and sustaining it. We assert that in using ESM, an organization will be able to define a desired state and develop a path to attain and sustain it.

Slide 17



Carnegie Mellon
Software Engineering Institute

Security Strategy Questions

What is to be protected?

Why does it need to be protected?
- What is the link to business drivers?
- Which security requirements are most important? Why?

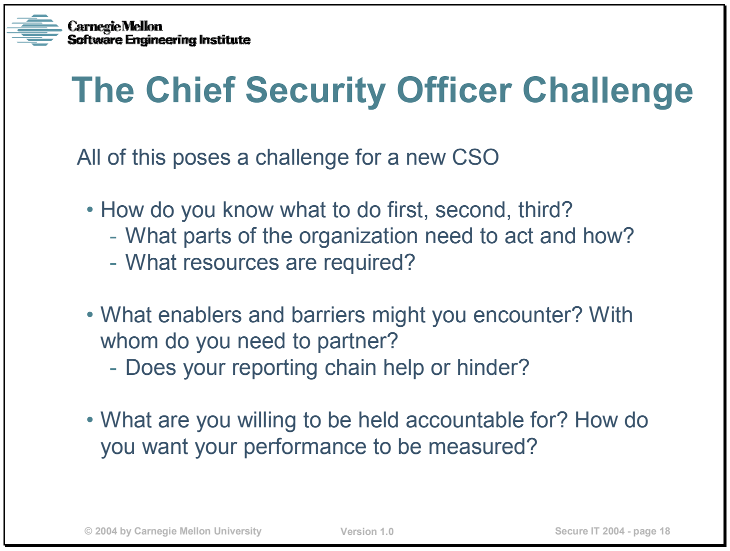
What happens if it is not protected?
- What is the organization’s risk tolerance?
- Which requirements, if unmet for any reason, would impact the enterprise? What is the organization’s impact tolerance?

Version 1.0

In formulating a security strategy, an organization needs to answer some tough questions. In the absence of answers to these questions (and a process for periodically updating them), an organization cannot define and deploy an effective security strategy.

Clearly, an organization cannot protect everything. So dialog and definition with respect to the organization’s ability to tolerate risk and ability to tolerate impact if the risk is realized are essential.

“The goal of security is to ensure the organization’s ability to grow and fulfill its mission in the face of a changing risk environment.” Security is an enabler of corporate strategy. Anish Bhimani. “How to Make Security Matter.” Information Security Magazine, August 2003. Available at http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss21_art101,00.html.



Carnegie Mellon
Software Engineering Institute

The Chief Security Officer Challenge

All of this poses a challenge for a new CSO

- How do you know what to do first, second, third?
  - What parts of the organization need to act and how?
  - What resources are required?
- What enablers and barriers might you encounter? With whom do you need to partner?
  - Does your reporting chain help or hinder?
- What are you willing to be held accountable for? How do you want your performance to be measured?

Here are some likely barriers for a new CSO or CISO who is faced with the problem described thus far:

You report to the CIO whose focus is on technology. What about problems that bleed into physical security and administrative issues?

You know that security is a business problem that must be actively managed, yet the organization thinks it is a technical specialty. They ask you not to stray into issues of business drivers, etc.

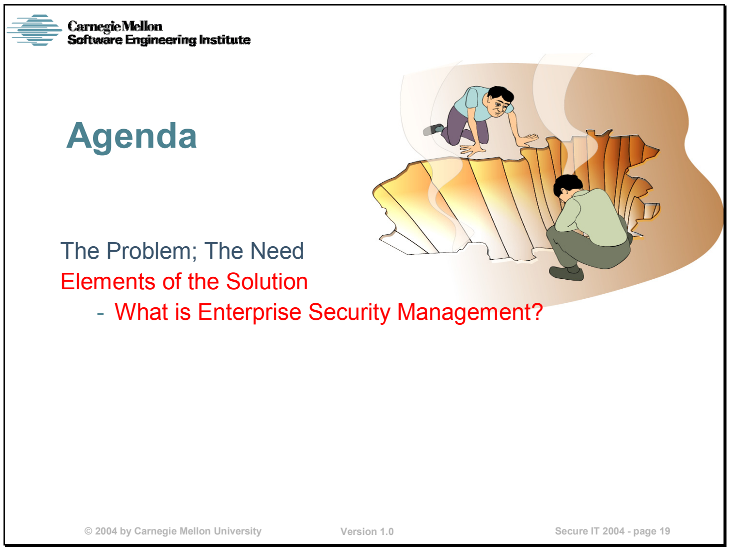
You know that to get your job done you will need to mobilize everyone to act and to expand their jobs horizontally to include security functions and capabilities. How do you influence other parts of the organization to act, given that don't report to you? How do you get them to work together? What are the incentives?

You must draw upon and expand the core competencies of the organization to achieve your objectives.

You have to make these other parts of the organization "care"

"The CSO's role is to enable business success in an appropriately secure context [James Christiansen, GM CISO]. When CISOs use too much of technology-centric, technology-first orientation, executives conclude that security is at a level that's inappropriate for their consideration. Building and maintaining strong relationships with business executives and their groups requires the CSO to assume a number of different guises: educator, strategist, negotiator, interpreter and, sometimes, disciplinarian." ["Information Protection Instead of IT Security."
http://www.csoonline.com/fundamentals/abc_leadership.html]

Slide 19



Carnegie Mellon
Software Engineering Institute

Agenda

The Problem; The Need
Elements of the Solution
- What is Enterprise Security Management?

© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 19

The objectives of information survivability and resiliency are essential elements of our evolving ESM approach. Here are two sources that further describe these concepts.

“Survivability is an emerging discipline that blends computer security with business risk management for the purpose of protecting highly distributed information services and assets. A fundamental assumption is that no system is totally immune to attacks, accidents, or failures. Therefore, the focus of this new discipline is not only to thwart computer intruders, but also to ensure that mission-critical functions are sustained and essential services are delivered, despite the presence of cyber attacks, failures, and accidents. Survivability solutions are best understood as risk-management strategies that first depend on the intimate knowledge of the mission being protected.”

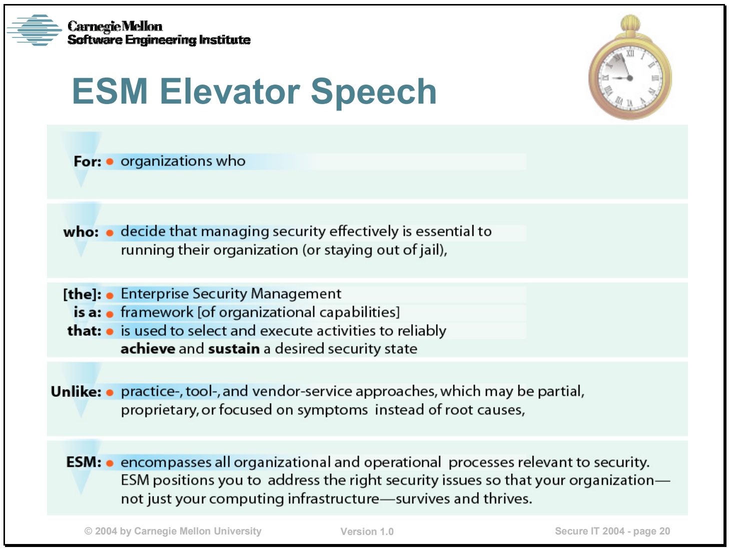
Lipson, Howard, Fisher, David. "Survivability - A New Technical and Business Perspective on Security." *Proceedings of the 1999 New Security Paradigms Workshop*. Association for Computing Machinery, 1999. Available at http://www.cert.org/archive/pdf/busperspec.pdf.

“Enterprise resilience is the ability and capacity to withstand systemic discontinuities and adapt to new risk environments. A resilient organization effectively aligns its strategy, operations, management systems, governance structure, and decision-support capabilities so that it can uncover and adjust to continually changing risks, endure disruptions to its primary earnings drivers, and create advantages over less adaptive competitors.

“A resilient organization establishes transparency and puts in place controls for CEOs and boards to address risks across the extended enterprise. It can withstand improper or fraudulent employee behavior, IT infrastructure failures, disruptions of interdependent supply chains or customer channels, intellectual property theft, adverse economic conditions across markets, and the myriad other discontinuities companies face today.”

Starr, Randy; Newfrock, Jim; Delurey, Michael. “Enterprise Resilience: Managing Risk in the Networked Economy.” strategy+business, Spring 2003. Also appears in “Enterprise Resilience: Risk and Security in the Networked World: A strategy+business Reader.” Randall Rothenberg, ed.

Slide 20



Carnegie Mellon
Software Engineering Institute

ESM Elevator Speech

For: • organizations who

who: • decide that managing security effectively is essential to running their organization (or staying out of jail),

[the]: • Enterprise Security Management
is a: • framework [of organizational capabilities]
that: • is used to select and execute activities to reliably **achieve** and **sustain** a desired security state

Unlike: • practice-, tool-, and vendor-service approaches, which may be partial, proprietary, or focused on symptoms instead of root causes,

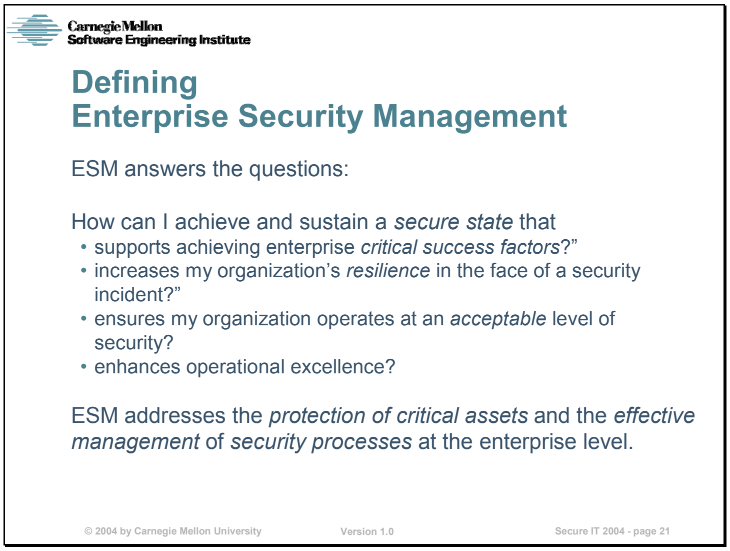
ESM: • encompasses all organizational and operational processes relevant to security. ESM positions you to address the right security issues so that your organization—not just your computing infrastructure—survives and thrives.

© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 20

ESM is as an emerging body of work that is focused on the effective management of security in an organization or enterprise. In other words, for organizations who realize that managing security effectively is essential to running their business or staying out of jail (given the growing body of international, federal/national, state, and local regulations and legislation), ESM is used to select, execute, and improve activities to reliably achieve and sustain a desired security state. Unlike practice- tool-, and vendor-service approaches, which may be partial, proprietary, or focused on symptoms instead of root causes, ESM encompasses all organizational and operational processes and participants relevant to security. ESM, when fully developed, will position an organization to address the right security issues so that the business—not just its computing infrastructure—survives and thrives.

The notion of an elevator speech comes from Geoffrey Moore in *Crossing the Chasm* (HarperBusiness, 2002). An elevator speech is targeted to the CEO, and is given in the time it takes to ride from the ground floor to the top floor. When properly formulated, it compels the CEO to take further action.

Slide 21



Defining Enterprise Security Management

ESM answers the questions:

How can I achieve and sustain a *secure state* that

- supports achieving enterprise *critical success factors*?”
- increases my organization’s *resilience* in the face of a security incident?”
- ensures my organization operates at an *acceptable* level of security?
- enhances operational excellence?

ESM addresses the *protection of critical assets* and the *effective management* of *security processes* at the enterprise level.

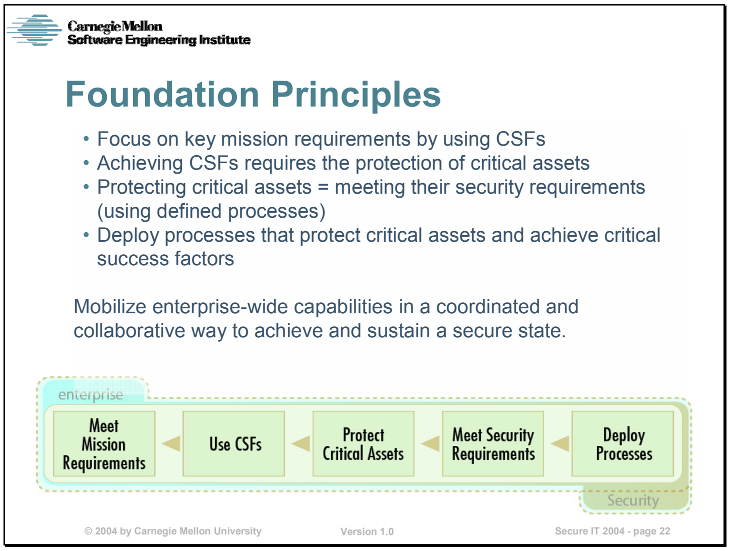
We are in the process of identifying key organizational and operational processes (and their interrelationships) that are essential to achieving and sustaining a desired state of security. When we say, “desired state of security” we mean that the security requirements of critical assets are met. Where they cannot be met, the residual risk is managed. Critical assets are those that contribute to achieving the mission and that can impact the mission if they are compromised (lost, stolen, disclosed, damaged).

Critical success factors are the limited number of areas in which satisfactory results will ensure competitive performance for the organization and enable it to achieve its mission. They typically reflect key areas of activities in which favorable results are necessary to achieve goals, where things must go right for the organization to flourish, and that should receive constant attention from management. [John F. Rockhart, “Chief Executives Define Their Own Data Needs,” Harvard Business Review, 1979]

Enterprise resilience is the ability and capacity to withstand systemic discontinuities and adapt to new risk environments.

An acceptable level of security is one where the investment in security protection strategies is commensurate with the risk of exposure to the assets being protected.

Slide 22



Carnegie Mellon
Software Engineering Institute

Foundation Principles

- Focus on key mission requirements by using CSFs
- Achieving CSFs requires the protection of critical assets
- Protecting critical assets = meeting their security requirements (using defined processes)
- Deploy processes that protect critical assets and achieve critical success factors

Mobilize enterprise-wide capabilities in a coordinated and collaborative way to achieve and sustain a secure state.

enterprise

Meet Mission Requirements ◄ Use CSFs ◄ Protect Critical Assets ◄ Meet Security Requirements ◄ Deploy Processes

Security

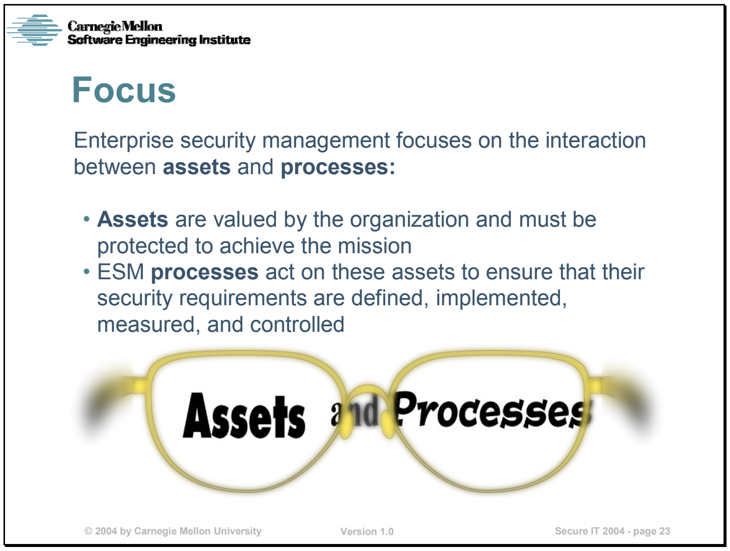
© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 22

We assert that all the right capabilities of an organization must mobilize [see slides 32-33] in a coordinated and collaborative way to achieve desired security goals. These security goals are reached by implementing, monitoring, and controlling the security requirements of critical assets, managing risks to these assets, and using effective processes to do so. Securing critical assets is necessary to achieve the organization’s critical success factors. Critical success factors must be performed consistently to achieve the organization’s mission.

The skills, capabilities, and efforts of the entire organization must be brought to bear. Key functions and processes must reflect and implement shared security goals and strategy. The organization’s security objectives or an articulation of the desired state must be developed and understood. Critical assets that are essential to achieving the organization’s mission must be identified and protected. There is a shared understanding of the organization’s drivers in the form of critical success factors.

The ultimate goal of enterprise security management is to ensure the protection of an organization’s critical assets through the implementation and improvement of security-relevant processes.

Slide 23



Focus

Enterprise security management focuses on the interaction between **assets** and **processes:**

- **Assets** are valued by the organization and must be protected to achieve the mission
- ESM **processes** act on these assets to ensure that their security requirements are defined, implemented, measured, and controlled

Assets
and
Processes

To achieve a secure state, an enterprise needs to address two artifacts: assets and processes relevant to the protection of assets.

An asset is anything of value to an organization. Assets include: information assets, technology assets, and supporting assets. An asset is described by its:

Characteristics (criticality; handling requirements including security and data classification; other attributes)

Content

Where it resides

How it is accessed and rules for same

Roles (sponsor, champion/advocate, owner, custodian, user, etc.)

Life cycle (creation/development, deployment (installation/rollout), use/operation, maintenance, retirement)

Relationships with other assets (parent, child, peer, other)

The processes that interact with it (uses, is used by, interfaces to/from)

A process is a systematic series of progressive and interdependent actions or steps by which an end result is obtained. A process is described by its:

Steps and interfaces between steps

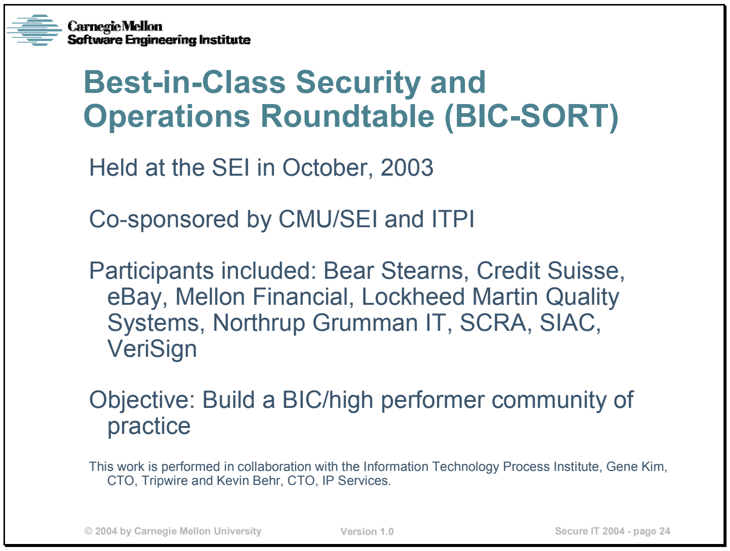
Roles (sponsor, champion/advocate, owner, custodian, user, etc.)

Life cycle (creation/development, deployment (installation/rollout), use/operation, maintenance, retirement)

Relationships with other processes (uses, is used by, interfaces to/from)

Relationships with assets (use, create, modify, delete)

Slide 24



Carnegie Mellon
Software Engineering Institute

Best-in-Class Security and Operations Roundtable (BIC-SORT)

Held at the SEI in October, 2003

Co-sponsored by CMU/SEI and ITPI

Participants included: Bear Stearns, Credit Suisse, eBay, Mellon Financial, Lockheed Martin Quality Systems, Northrup Grumman IT, SCRA, SIAC, VeriSign

Objective: Build a BIC/high performer community of practice

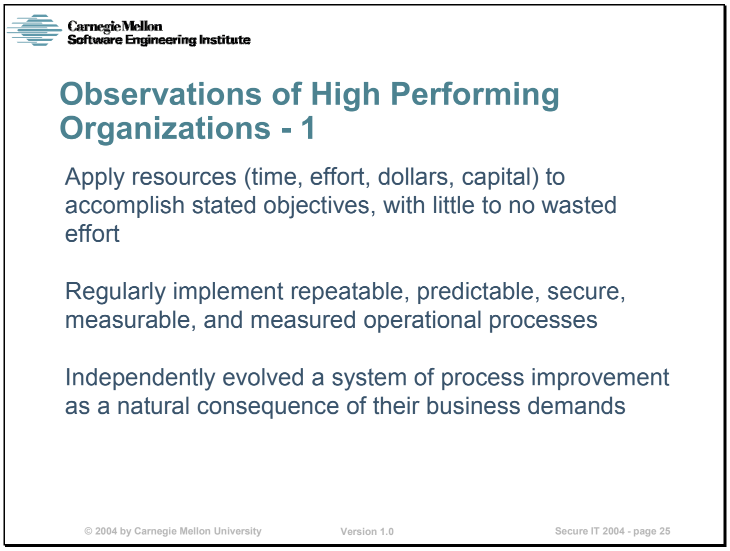
This work is performed in collaboration with the Information Technology Process Institute, Gene Kim, CTO, Tripwire and Kevin Behr, CTO, IP Services.

Version 1.0

Among the stated goals of this event were to begin to build an executive-level community of practice for IT (information technology) operations and security, with a common sense of purpose and a desire to influence other relevant and connected communities of practice; and to better capture and articulate the relevant bodies of knowledge that enable and accelerate IT operational and security process improvement. Since then, we have been actively synthesizing and augmenting the data we collected.

The workshop proceedings are available in a report published by the SEI: Allen, Julia, et al. *Best in Class Security and Operations Round Table Report* (CMU/SEI-2004-SR-002). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, March 2004. Copies of the report are available upon request.

Slide 25



Carnegie Mellon
Software Engineering Institute

Observations of High Performing Organizations - 1

Apply resources (time, effort, dollars, capital) to accomplish stated objectives, with little to no wasted effort

Regularly implement repeatable, predictable, secure, measurable, and measured operational processes

Independently evolved a system of process improvement as a natural consequence of their business demands

How do you know a high performing organization when you see it? Can you walk into an organization and determine within 15 minutes if they are high performing or not?

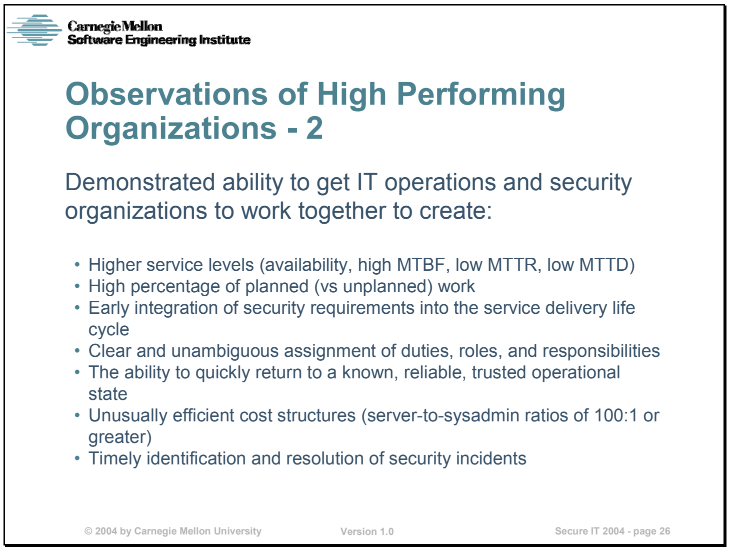
High performing (HP) security and IT operations organizations are effective and efficient. They successfully apply resources (time, effort, dollars, capital) to accomplish stated objectives, with little to no wasted effort. They regularly implement repeatable, predictable, defined, secure, measurable, and measured operational processes. These organizations have evolved a system of process improvement as a natural consequence of their business demands.

High performing organizations successfully balance IT operational risks and controls. This balance and the practices that implement it directly map to organizational business drivers by increasing operational availability and security. High performing organizations invest in pre-release activities such as release management processes.

They value and use controls to improve efficiency and effectiveness, for example, by detecting production variances early (so as to incur the lowest cost and least impact). Controls-based auditing requires that preventive, detective, and corrective controls are in place. In HP organizations, auditable controls are visible and easily inspected. HP organizations use these controls to help ensure consistent practice necessary to achieve business goals (that rely on mature IT operations and security processes). As a result, HP organizations require considerably less effort to meet management's and audit's expectations and requirements. External auditors/consultants recognize operational excellence in such organizations.

“People in high performing IT organizations don’t feel different from other corporate citizens; in fact, they are business savvy leaders in their own right. They operate according to the same corporate values as everyone else and are measured by the same tough performance standards.” [Charlie Feld, Donna Stoddard. “Getting IT Right.” Harvard Business Review, February 2004, page 78.]

Slide 26



Carnegie Mellon
Software Engineering Institute

Observations of High Performing Organizations - 2

Demonstrated ability to get IT operations and security organizations to work together to create:

- Higher service levels (availability, high MTBF, low MTTR, low MTTD)
- High percentage of planned (vs unplanned) work
- Early integration of security requirements into the service delivery life cycle
- Clear and unambiguous assignment of duties, roles, and responsibilities
- The ability to quickly return to a known, reliable, trusted operational state
- Unusually efficient cost structures (server-to-sysadmin ratios of 100:1 or greater)
- Timely identification and resolution of security incidents

Version 1.0

Results of informal benchmarking indicate that high performing IT operations and security organizations work together to create

higher service levels (high availability/uptime/mean time between failures, low mean time to detect problems/incidents, low mean time to repair) and rigorously defined service level agreements

a high percentage of planned, scheduled work (vs. unplanned work)

earliest integration of information security requirements in the service delivery life cycle

clear and unambiguous assignment of duties, roles, and responsibilities

the ability to quickly return to a known, reliable, trusted operational state when problems arise with a new change or configuration

unusually efficient cost structures (server-to-system administrator ratios of 100:1 or above as contrasted with an order of magnitude less in most organizations)

timely identification and resolution of security incidents

a high percentage of time spent in proactive (vs. reactive) mode

productive working relationship with peers (smooth audits, streamlined governance)

an ability to devote increasingly more time and resources to strategic issues, having mastered tactical concerns

Indicators of the absence of high performing behavior include obvious dysfunction such as

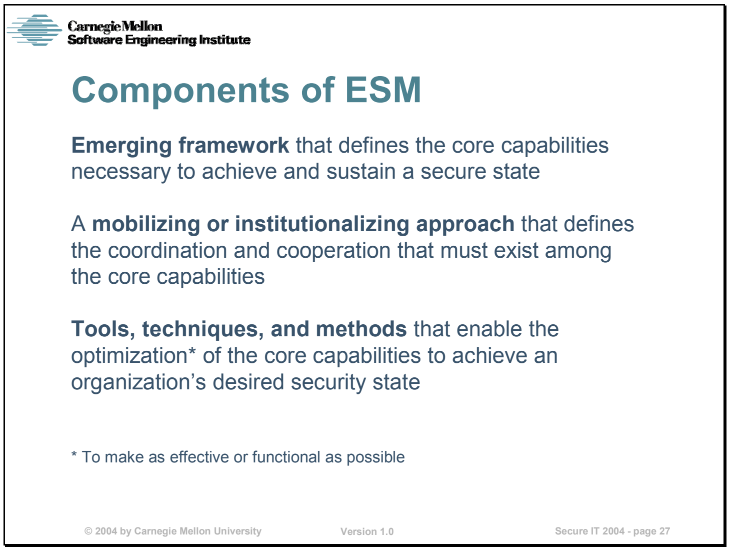
a high degree of thrashing; an attitude that “things just keep happening to us” and “lots of energy is lost in the system”

ineffective interfaces with peers (research and development, application developers, audit, security, operations) that get in the way of getting things done

a high percentage of time spent on reactive tasks

lack of metrics and their use to inform decision making

Slide 27



Carnegie Mellon
Software Engineering Institute

Components of ESM

Emerging framework that defines the core capabilities necessary to achieve and sustain a secure state

A **mobilizing or institutionalizing approach** that defines the coordination and cooperation that must exist among the core capabilities

Tools, techniques, and methods that enable the optimization* of the core capabilities to achieve an organization's desired security state

* To make as effective or functional as possible

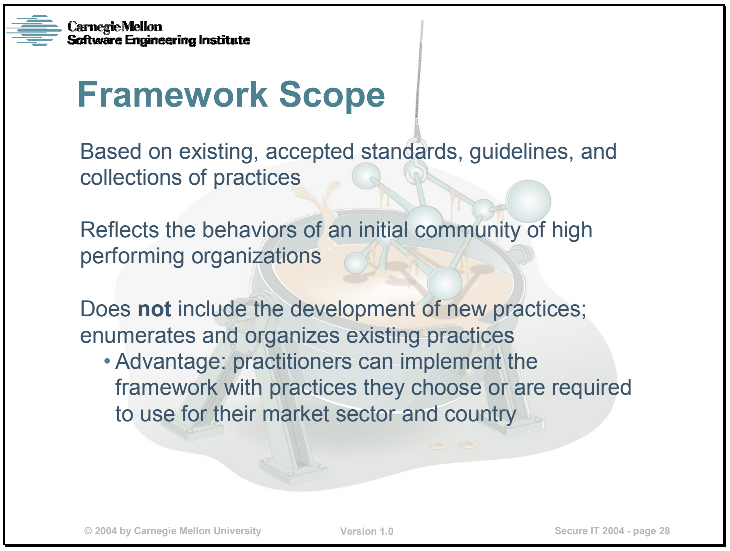
Version 1.0

Enterprise security management, as we currently envision it, includes a framework that defines and articulates the enterprise capabilities that must collectively be brought to bear to achieve and sustain a secure state. This framework draws from a wide range of existing, credible, and reputable sources. The framework and its evolution are further described in the following slides.

The mobilizing approach describes how these capabilities need to interact, the information that is shared among them, the processes that define the interaction and information flow, and, eventually, candidate scenarios for navigating the framework.

We have begun to identify a promising set of tools, techniques, and methods that may aid in implementation. One of these (undesirable effects analysis) is detailed in slides 36-41 and directly results from the BIC SORT event and follow up synthesis with Gene Kim and Kevin Behr. Several others (Observations/Hypotheses, CMMI process areas, Six Sigma, and Critical Success Factors) are briefly covered in the backup slides (45-57). We will continue to develop and add to this list.

Slide 28


Carnegie Mellon
Software Engineering Institute

Framework Scope

Based on existing, accepted standards, guidelines, and collections of practices

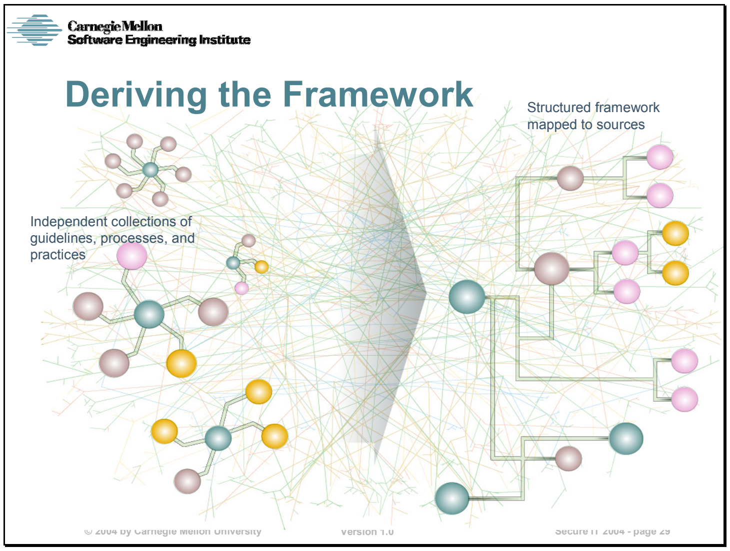
Reflects the behaviors of an initial community of high performing organizations

Does **not** include the development of new practices; enumerates and organizes existing practices

- Advantage: practitioners can implement the framework with practices they choose or are required to use for their market sector and country

In defining the framework, we draw from a set of community-accepted standards, regulations, guidelines, reports, assessment instruments, checklists, and best practices. In addition, we draw from our continued observation of and work with high performing organizations (along with continuing to evolve the definition of what high performing means).
We do not intend to develop new processes or practices unless we identify obvious gaps. Even in this case, we will likely turn to a knowledgeable and reputable community of practice to identify additional sources. The intent is to map to all named sources but not duplicate them, such that any organization can use the framework and select those that are most applicable for their market sector and critical success factors. By using a unifying framework that is fully mapped, we are hopeful that organizations can more easily demonstrate satisfaction of current and emerging information security requirements.

Slide 29



Carnegie Mellon
Software Engineering Institute

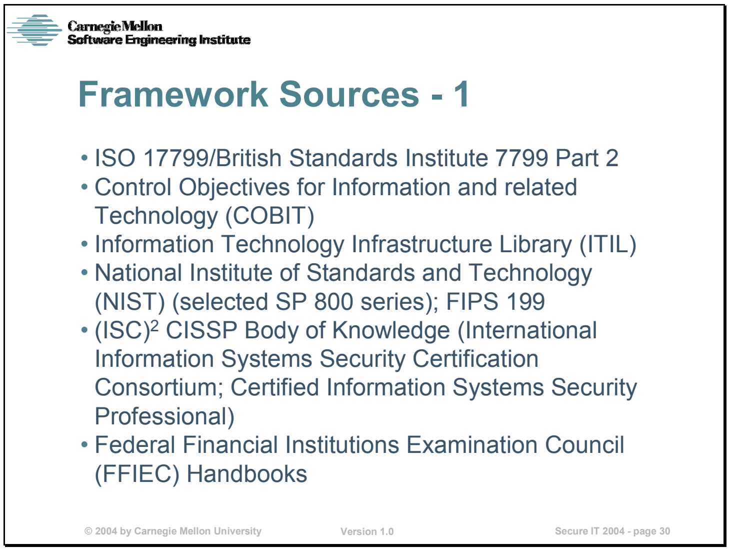
Deriving the Framework

An initial analysis of several widely accepted and used sources (specifically ISO 17799, COBIT, ITIL, and selected NIST 800 series special publications) led us to a set of eight top level capability areas, shown on slide 32. We are now in the process of verifying these grouping by cross referencing against additional sources shown in the next two slides. Again, the intent is to provide a navigational aid and framework for many of the leading sources that are being used today as well as an ability to map those that emerge in the future.

Our desired outcome is to articulate a framework (with references to practice-specific behaviors) that draw from all of the bodies of knowledge in each of the capability areas. Many of these exist today but they are all stove piped and most often intended for a narrowly defined constituency (system administrators, auditors, security staff, middle managers, senior managers). We intend to integrate these capabilities across an enterprise to bring the knowledge and skills of each to bear to assist organizations in achieving and sustaining a well defined security state.

In some high performing organizations, we find the presence of an enterprise architecture (that may include process models, policies, standards, standard operating procedures). This architecture defines how the organization does business at a fairly detailed operational level. When such an organization chooses to adopt a new standard, regulation, or quality model, a small team is able to map the new requirements to the existing architecture, make required changes in accordance with a defined improvement process, and thereby demonstrate ‘compliance’ with relatively minor impact on the organization at large. We are hopeful that this framework can evolve to provide this type of utility for organizations lacking a standard approach.

Slide 30



Carnegie Mellon
Software Engineering Institute

Framework Sources - 1

- ISO 17799/British Standards Institute 7799 Part 2
- Control Objectives for Information and related Technology (COBIT)
- Information Technology Infrastructure Library (ITIL)
- National Institute of Standards and Technology (NIST) (selected SP 800 series); FIPS 199
- (ISC)^2 CISSP Body of Knowledge (International Information Systems Security Certification Consortium; Certified Information Systems Security Professional)
- Federal Financial Institutions Examination Council (FFIEC) Handbooks

Version 1.0

This list is drawn from a wide range of accepted, credible, reputable national and international sources, synthesizing from existing bodies of work and considering case studies. We are also relying on the collective research and field experience of the Networked Systems Survivability program and others at the Software Engineering Institute in the implementation and adoption of a wide range of software engineering improvement initiatives.

For a related discussion comparing and contrasting popular quality models, see Gary Anthes. “Quality Model Mania.” Computerworld, March 8, 2004, available at http://www.computerworld.com/developmenttopics/development/story/0,10801,90797,00.html. The article addresses CMM, COBIT, ITIL, Six Sigma, ISO 9000, and Malcolm Baldrige

Framework sources:

British Standards Institution (BSI). IT Service Management Part 1: Specification for service management (BS 15000-1:2002), 27 September 2002. Part 2: Code of practice for service management (BS 15000-2:2003), 22 January 2003

COBIT 3rd Edition Executive Summary, Framework, Control Objectives, and Management Guidelines, July 2000. Available at http://www.itgi.org and http://www.isaca.org

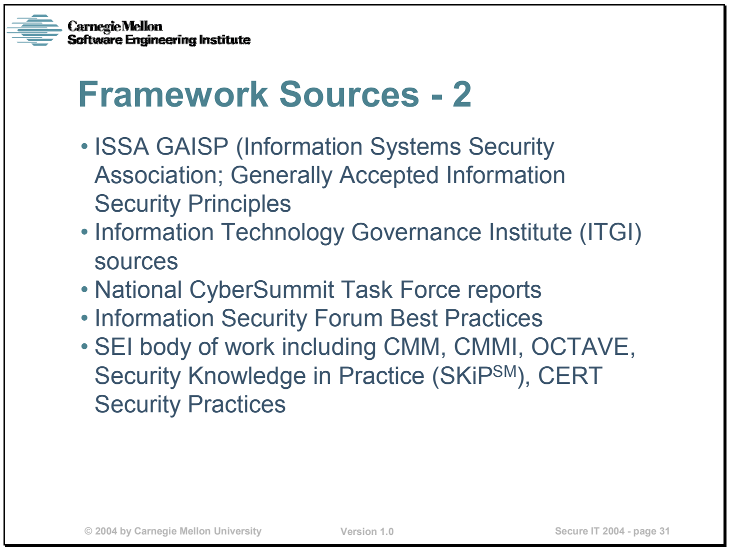
Information Technology Infrastructure Library (ITIL) ® . Office of Government Commerce. Refer to http://www.ogc.gov.uk/index.asp?id=2261 and http://www.itsmf.com

U.S. National Institute for Standards and Technology. Special Publications, 800 Series. Available at http://csrc.nist.gov/publications/nistpubs/

Hansche, Susan; Berti, John; Hare, Chris. *Official (ISC)2® Guide to the CISSP® Exam*. Auerbach Publications, 2004.

Federal Financial Institutions Examination Council. IT Examination Handbooks. Available at http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html

Slide 31



Framework Sources - 2

- ISSA GAISP (Information Systems Security Association; Generally Accepted Information Security Principles
- Information Technology Governance Institute (ITGI) sources
- National CyberSummit Task Force reports
- Information Security Forum Best Practices
- SEI body of work including CMM, CMMI, OCTAVE, Security Knowledge in Practice (SKiP^{SM}), CERT Security Practices

Framework Sources (cont.):

Information Systems Security Association. Generally Accepted Information Security Principles. Available at http://www.issa.org/gaisp/gaisp.html

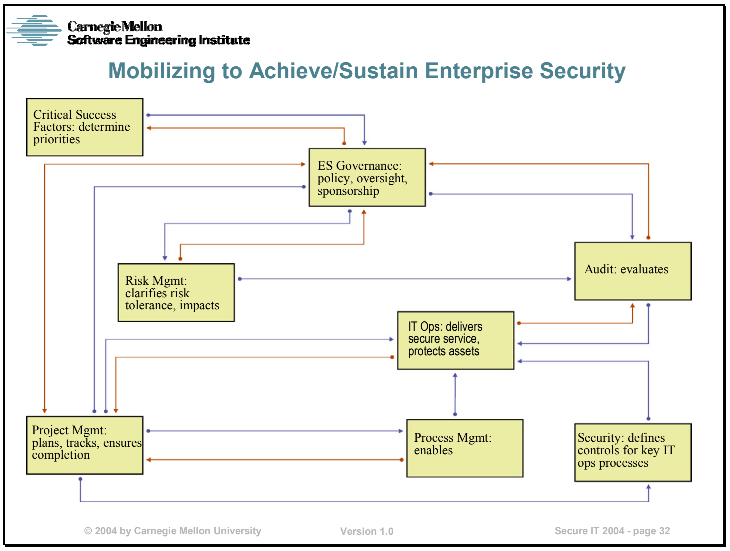
IT Governance Institute. “Board Briefing on IT Governance.” Information Systems Audit and Control Foundation, 2001. Available at http://www.itgovernance.org/resources.htm

IT Governance Institute. “Information Security Governance: Guidance for Boards of Directors and Executive Management.” Information Systems Audit and Control Foundation, 2001. Available at http://www.itgovernance.org/resources.htm

National Cyber Security Partnership. Task Force Reports. Available at http://www.cyberpartnership.org

Information Security Forum. “The Standard of Good Practice for Information Security.” March 2003. Available at http://www.isfsecuritystandard.com/index_ns.htm

Slide 32



Carnegie Mellon
Software Engineering Institute

Mobilizing to Achieve/Sustain Enterprise Security

Critical Success Factors: determine priorities

ES Governance: policy, oversight, sponsorship

Risk Mgmt: clarifies risk tolerance, impacts

Audit: evaluates

IT Ops: delivers secure service, protects assets

Project Mgmt: plans, tracks, ensures completion

Process Mgmt: enables

Security: defines controls for key IT ops processes

© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 32

As currently envisioned, mobilizing an enterprise to achieve and sustain a desired security state involves eight integrated capabilities as shown above. We call these Capability Areas (CA):

The identification and use of critical success factors to determine priorities that derive from business objectives

Enterprise security (ES) governance to define and enforce policy, ensure regular oversight and review, and enact visible sponsorship that establishes the enterprise culture with respect to security (such as security is important to each and every user)

Risk management to articulate the organization’s risk tolerance and identify and manage ES risks to critical assts

Audit to evaluate the enterprise’s current security state against established criteria

Project management to identify, track, and successfully bring to closure ES-related projects. Each project enacts some change desired by the organization.

Process management to define and mature ES process definitions as well as IT processes that implement security controls

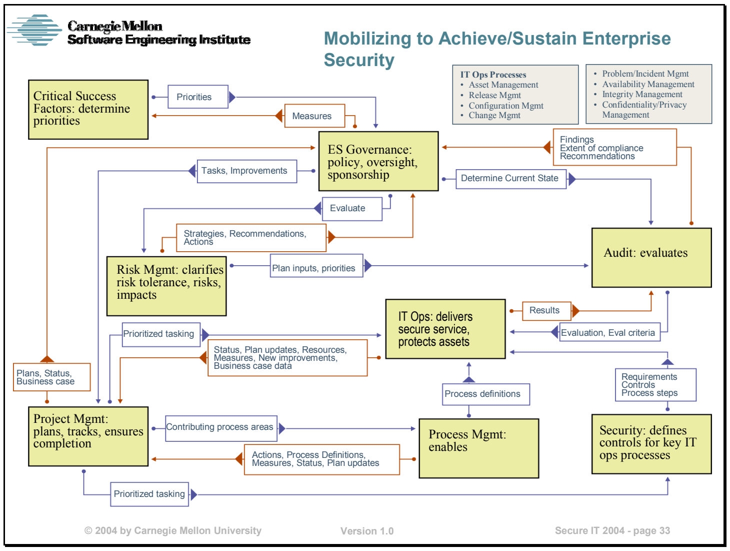
IT operations to provide a robust, flexible operational infrastructure that meets enterprise security requirements (confidentiality, availability, integrity, privacy, authentication, non-repudiation) by protecting critical assets, delivering secure services, and implementing security controls

Security to define controls for IT operational processes that, when implemented, cause security requirements to be met (test: the presence of an effectively implemented and measured control is adequate demonstration that a security requirement is met)

The top four capability areas (Critical Success Factors, ES Governance, Risk Management, Audit) provide oversight and top level management. Governance and audit serve as enablers and accelerators. CSFs serve as the explicit link to business drivers to ensure that value is being delivered at this level.

The bottom four capability areas (Project Management, Process Management, IT Operations, Security) provide detailed management and execution in accordance with the policies, procedures, and guidelines established by senior management. Project management is applied to all IT operations changes, updates, and new applications, and actively supports IT portfolio management as it relates to security. Process management is conducted in accordance with the SEI’s CMMI model. IT operations and security are held to corporate performance standards, as for any other business unit. Business unit managers are project managers for IT/security projects on which they rely.

Slide 33



Carnegie Mellon
Software Engineering Institute

Mobilizing to Achieve/Sustain Enterprise Security

IT Ops Processes
- Asset Management
- Release Mgmt
- Configuration Mgmt
- Change Mgmt

- Problem/Incident Mgmt
- Availability Management
- Integrity Management
- Confidentiality/Privacy Management

Critical Success Factors: determine priorities

Priorities

Measures

ES Governance: policy, oversight, sponsorship

Findings
Extent of compliance
Recommendations

Tasks, Improvements

Determine Current State

Evaluate

Strategies, Recommendations, Actions

Risk Mgmt: clarifies risk tolerance, risks, impacts

Plan inputs, priorities

Audit: evaluates

IT Ops: delivers secure service, protects assets

Results

Evaluation, Eval criteria

Prioritized tasking

Status, Plan updates, Resources, Measures, New improvements, Business case data

Plans, Status, Business case

Process definitions

Requirements
Controls
Process steps

Project Mgmt: plans, tracks, ensures completion

Contributing process areas

Process Mgmt: enables

Security: defines controls for key IT ops processes

Actions, Process Definitions, Measures, Status, Plan updates

Prioritized tasking

Version 1.0

This more detailed version of the mobilizing diagram begins to show some of the key interfaces and information flow.

Some of the connections that we are currently examining include:

Using contributing process areas and process definitions from the SEI's CMMI. These include risk management, project management, and process management. There may be some overlap between audit and CMMI's process and product quality assurance process area.

Selected processes used to manage IT operations appear promising as productive mechanisms for security process/controls insertion and adoption. As a result, these controls (and the companion thinking about them) can become part of normal day-to-day operations. Based on work done by Gene Kim and Kevin Behr, ITIL, and our own work, the following specific IT operational processes appear the most promising:

Release management: ensure predictability of what goes into the operational environment

Configuration and change management: ensure changes are planned, tracked to authorized work orders, and explicitly scheduled in the operational environment

Problem and incident management: deal with problems efficiently and feed results back into affected processes. Note that incidents are treated as a class of problem.

Availability management: ensure that the infrastructure (collectively and at a component level) meets uptime requirements

Automation: do all of the above in an automated fashion, to the extent possible. A key automation concept is that of a repeatable, automated build system and supporting processes that provision (configure) what the enterprise wants to deploy.

Next steps currently in development:

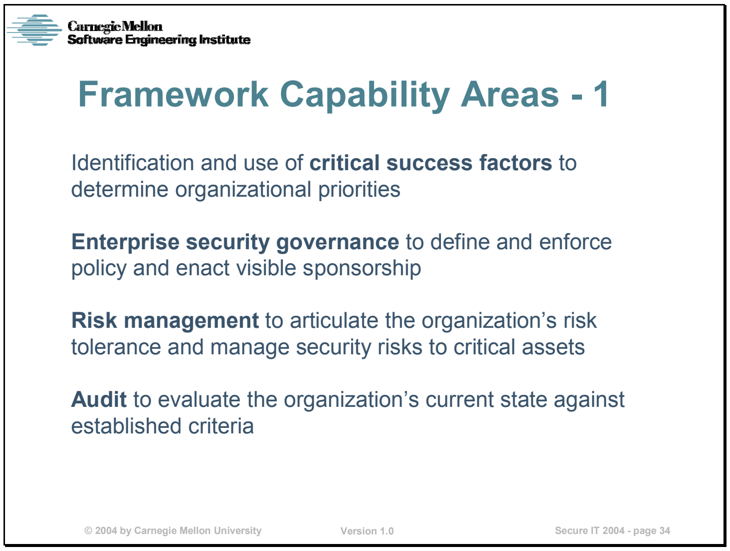
Develop scenarios that further detail how each of the capability areas interact

Identify a maturation approach for selected operational processes, building on the community's CMM, CMMI, and other software process improvement experiences. Include process objectives and measures.

Understand the role that ES governance, audit, and risk management can play as enablers to accelerate process maturation and adoption. There is emerging work in this area as well as in the area of IT security governance.

A recent project management survey indicates that organizations with more mature process models have an average cost/schedule deviation < 8% of the original prediction (due to improved accuracy in predicting and planning) as contrasted with typical variances of more than 200%. [Gary Richardson, Blake Ives (University of Houston). "Managing Systems Development." IEEE Computer, March 2004, pages 93-94.]

Slide 34



Carnegie Mellon
Software Engineering Institute

Framework Capability Areas - 1

Identification and use of **critical success factors** to determine organizational priorities

Enterprise security governance to define and enforce policy and enact visible sponsorship

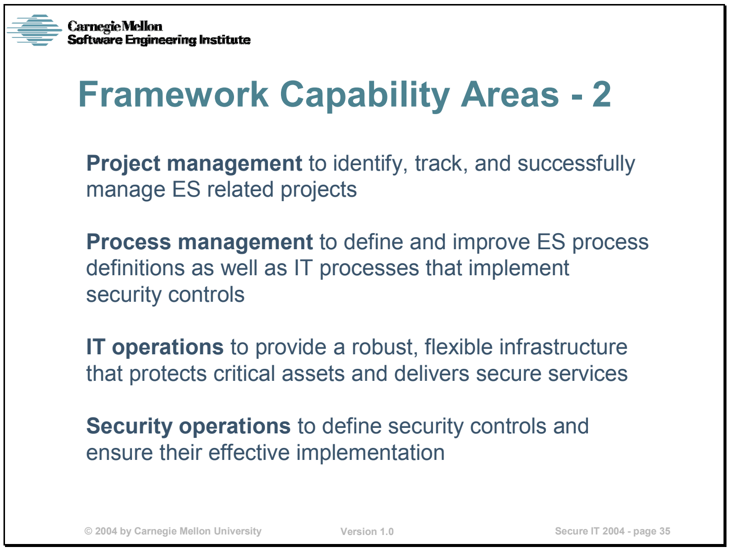
Risk management to articulate the organization’s risk tolerance and manage security risks to critical assets

Audit to evaluate the organization’s current state against established criteria

Version 1.0

This slide provides descriptions in support of the mobilizing framework.

Slide 35



Carnegie Mellon
Software Engineering Institute

Framework Capability Areas - 2

Project management to identify, track, and successfully manage ES related projects

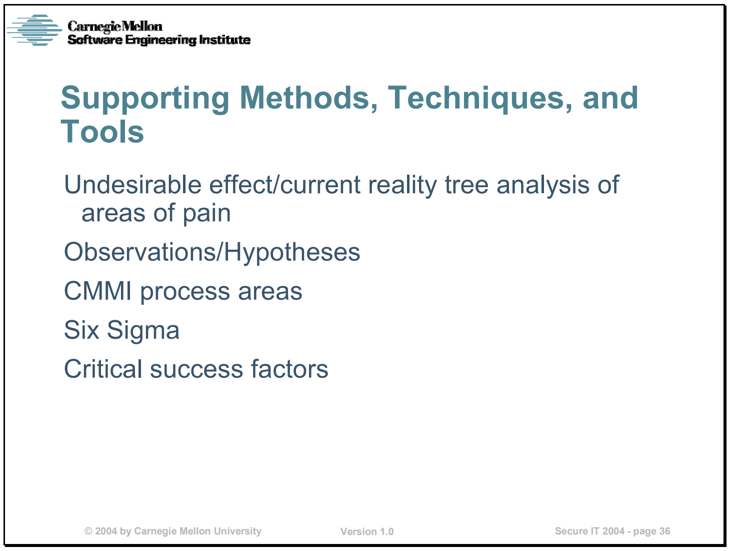
Process management to define and improve ES process definitions as well as IT processes that implement security controls

IT operations to provide a robust, flexible infrastructure that protects critical assets and delivers secure services

Security operations to define security controls and ensure their effective implementation

This slide provides descriptions in support of the mobilizing framework.

Slide 36



Carnegie Mellon
Software Engineering Institute

Supporting Methods, Techniques, and Tools

Undesirable effect/current reality tree analysis of areas of pain

Observations/Hypotheses

CMMI process areas

Six Sigma

Critical success factors

© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 36

We have begun to identify a promising set of tools, techniques, and methods that may aid in implementing the mobilizing framework. We will describe the results of our undesirable effect/current reality tree analysis in some detail in the following slides.

Several other approaches (Observations/Hypotheses, CMMI process areas, Six Sigma, and Critical Success Factors) are briefly covered in the backup slides (45-57). For example, Six Sigma methods can be used to reduce the number of successful incidents by reducing variance on the processes that detect and respond to intrusions. Reducing variances can produce results such as

increasing the number of incidents prevented

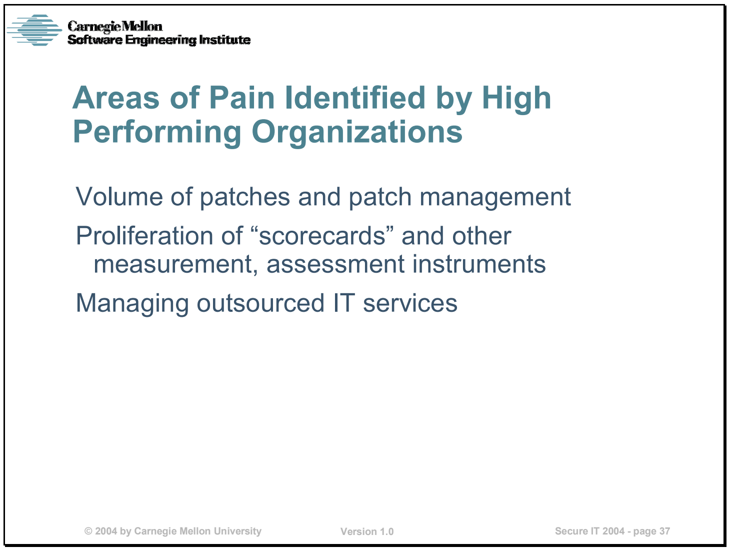
increasing the number of incidents detected by reducing the mean time to detect

reducing incident response times

reducing system restore times after an incident

We will continue to develop and add to this list.

Slide 37



Carnegie Mellon
Software Engineering Institute

Areas of Pain Identified by High Performing Organizations

Volume of patches and patch management

Proliferation of “scorecards” and other measurement, assessment instruments

Managing outsourced IT services

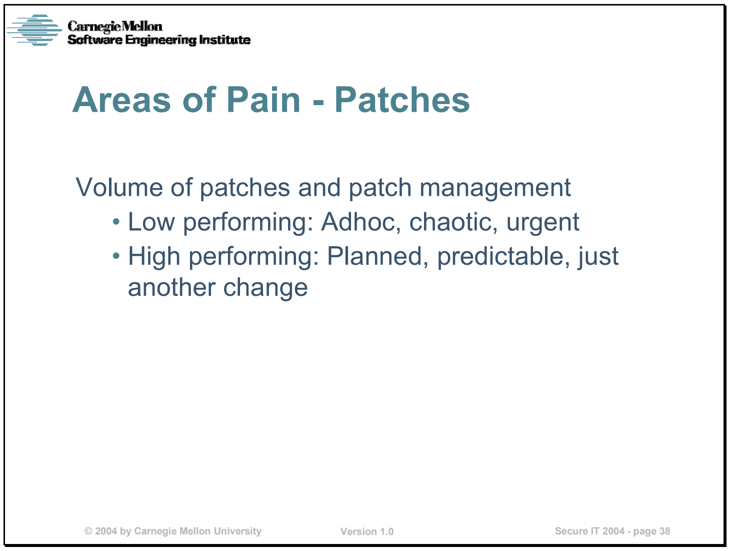
Version 1.0

During our BIC SORT event (October 2003; slides 24-26), we elicited areas of pain that participants are currently experiencing in their IT operations and security work. We captured almost fifty specific areas of pain in a range of organization and technology categories. We chose three of the most acute these to analyze further: keeping up with patches/patch management, dealing with the proliferation of management scorecards and other measurement and assessment instruments, and managing outsourced IT services.

To analyze these problems, we used a technique pioneered by Dr. Eliyahu Goldratt called the Theory of Constraints Thinking Tools, specifically problem clouds and current reality trees (for more information, see http://www.thedecalogue.com/Tools/crt.htm). The goal was to understand the causal factors and beliefs that led to both high- and low-performing behaviors, and then to identify common root causes among the three pain areas.

The notes that accompany slides 37-41 are summarized from Kim, Gene and Allen, Julia. “High-Performing IT Organizations: What You Need to Change to Become One.” Better Management.com, April 2004. Available at http://www.bettermanagement.com/Library/Library.aspx?a=13&LibraryID=9429.

Slide 38



Carnegie Mellon
Software Engineering Institute

Areas of Pain - Patches

Volume of patches and patch management

- Low performing: Adhoc, chaotic, urgent
- High performing: Planned, predictable, just another change

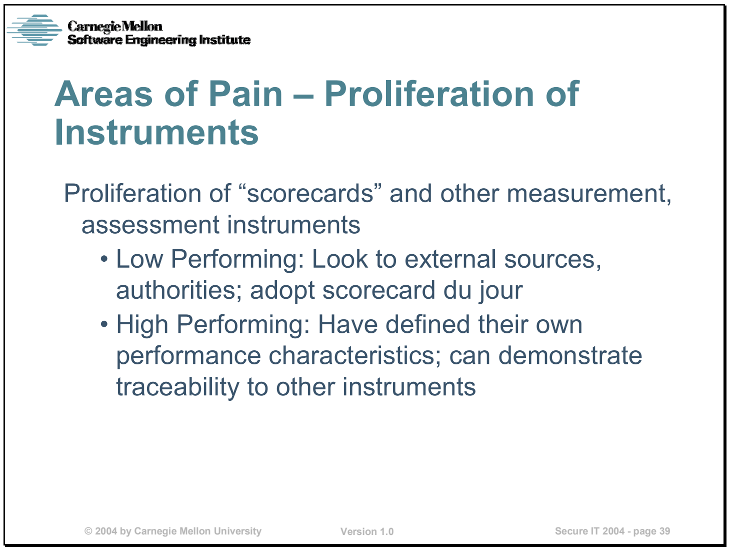
© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 38

An area of pain articulated by many of the participants at the BIC SORT was the volume of urgent patches needing to be applied to the operational infrastructure, resulting from the constant stream of new security vulnerabilities, and the need to find an effective solution to managing patches.

In low performing organizations, this activity is characterized as ad hoc, chaotic, and urgent. Announcement of the availability of a patch to address a critical security vulnerability leads to widespread chaos and disruption, often resulting in massive amounts of unplanned work at the expense of planned work. Worse, even successfully deploying the patch often causes unintended consequences, such as servers becoming non-functional or even unable to boot.

In contrast, high performers address patching as a predictable and planned activity, treating each patch as just another change. Announcement of critical patches result in merely adding the patch to the release engineering candidate queue, where it is evaluated, tested and integrated into an already scheduled release deployment. The absence of urgency and a well-defined process for integrating changes leads to a much higher change success rate. Interestingly, virtually all of the high-performers apply patches much less frequently than the low-performers, perhaps by one or two orders of magnitude, accepting the risk of the vulnerability exposure as less than the risk to availability due to unanticipated impacts of a bad or out of cycle change.

Slide 39



Carnegie Mellon
Software Engineering Institute

Areas of Pain – Proliferation of Instruments

Proliferation of “scorecards” and other measurement, assessment instruments

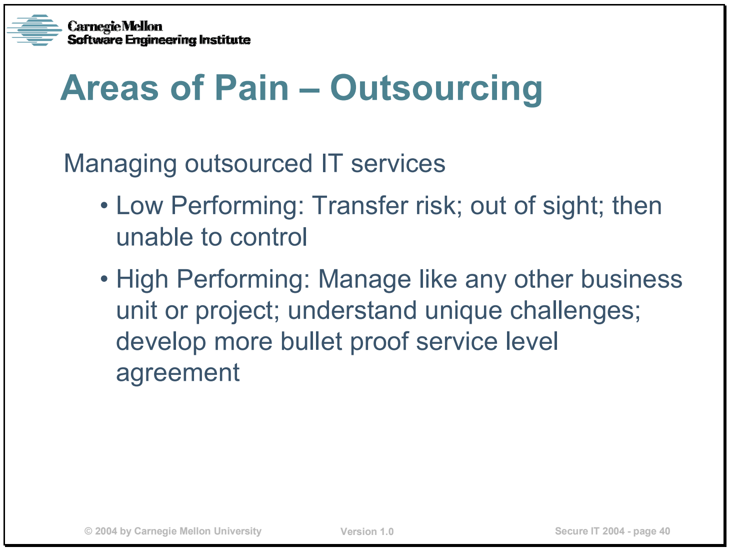
- Low Performing: Look to external sources, authorities; adopt scorecard du jour
- High Performing: Have defined their own performance characteristics; can demonstrate traceability to other instruments

BIC SORT participants listed the proliferation of IT management “scorecards” and other management and assessment instruments as another area of pain. We added into this category many of the current and emerging regulations, including Sarbanes-Oxley Section 404, Gramm-Leach-Bliley, and HIPAA.

For low performers, this activity is characterized by having to look to external sources and authorities for the desired behaviors and measurements. The absence of a strong internal IT management framework and belief system can lead to adopting a “scorecard du jour,” or worse, using multiple external scorecards simultaneously that conflict with each other. This can lead to more work/re-work for the organization, and excess retrofitting to deal with the necessary process and organizational changes in direction. Worse, executive turnover can result in switching scorecards, which sustains the chaos.

In contrast, high performers have their own clearly defined performance goals and desired characteristics. If the need to conform to an external scorecard or regulatory requirement materializes, they assign a small team to trace to it and make any necessary changes or enhancement. Consequently, they have a lower cost of developing, sustaining and documenting controls, a better posture of audit and compliance, and have little need to look externally for authorities to tell them how they need to operate.

Slide 40



Carnegie Mellon
Software Engineering Institute

Areas of Pain – Outsourcing

Managing outsourced IT services

- Low Performing: Transfer risk; out of sight; then unable to control
- High Performing: Manage like any other business unit or project; understand unique challenges; develop more bullet proof service level agreement

Version 1.0 Secure IT 2004 - page 40

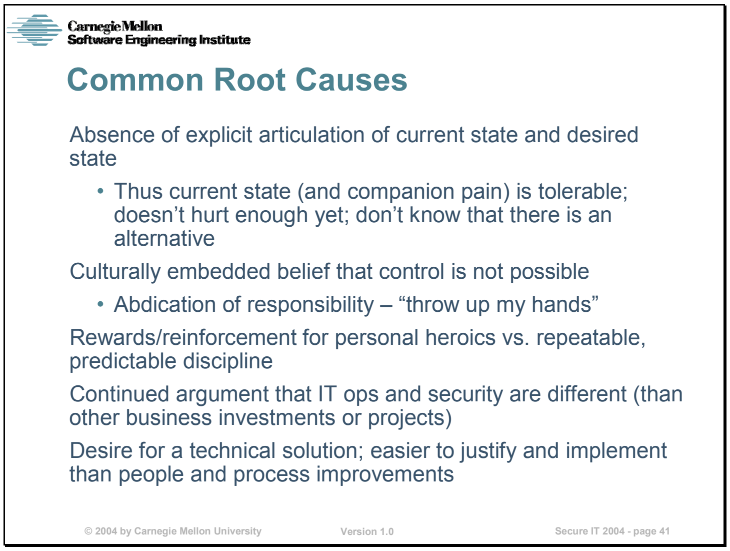
The last area of pain we analyzed was the challenge of managing outsourced IT services. Any challenges with IT are inherently made more complex when these services are provided by an outside organization instead of an employee: corrective actions may have contractual implications, the scope of corrections may be constrained by the service level agreement, and so forth.

In low performing organizations, there is often a desire to transfer the IT risk and responsibilities to someone else, especially if management perceives an absence of internal skills to meet business objectives. However, outsourced services rapidly become ‘out of sight and out of mind,’ until the organization finds that service levels are unacceptable and the client organization is unable to attest to the controls implemented by the service provider. The organization then discovers that it may have inadvertently exacerbated the challenges by outsourcing but unfortunately, bringing the services back in-house may no longer be an option.

In contrast, high performers manage outsourced IT services just like any other business unit or project. They understand the unique positive and negative challenges of providing IT projects or services by an external party. As a result, they develop more collaborative partnerships with long term providers, more bullet-proof service level agreements, and incentivize providers to improve service levels and capabilities to both parties benefit.

“The damage from mismanaged outsourcing will always exceed the potential benefits from anticipated IT cost reductions.” Strassman, Paul. “Most Outsourcing Is Still for Losers.” ComputerWorld, February 2, 2004. Available at http://www.computerworld.com/careertopics/careers/story/0,10801,89533,00.html.

Slide 41



Carnegie Mellon
Software Engineering Institute

Common Root Causes

Absence of explicit articulation of current state and desired state
- Thus current state (and companion pain) is tolerable; doesn't hurt enough yet; don't know that there is an alternative

Culturally embedded belief that control is not possible
- Abdication of responsibility – "throw up my hands"

Rewards/reinforcement for personal heroics vs. repeatable, predictable discipline

Continued argument that IT ops and security are different (than other business investments or projects)

Desire for a technical solution; easier to justify and implement than people and process improvements

© 2004 by Carnegie Mellon University   Version 1.0   Secure IT 2004 - page 41

After analyzing the three areas of pain, we started looking for common patterns and root causes that led to the preservation of the status quo in the low performers, despite the clear promise of alleviating the pain through achieving the characteristics of the high performers. We identified five initial root causes:

1. The absence of an explicit articulation of current state and desired state: Management concludes that the current state, along with all of the companion pains, is tolerable. These organizations may articulate a litany of pains and frustrations, but in the absence of being able to quantify the pain, may decide that it probably does not hurt enough yet to warrant any corrective action, or don't know what corrective action to take. This may be because of a sincere belief that the pain is not high enough yet, or it may be due to the next root cause.

A culturally embedded belief that control is not possible: Management may not know that there is an alternative, believing that control is not possible

due to the nature of IT and security ("IT operational and security issues are like the weather. There is nothing we can do about it and bad things happen to us, just like rain or hurricanes.")

due to business needs ("My business environment is too dynamic to accommodate bureaucratic processes or controls.")

as a result of a deliberate, or even unintentional, abdication of responsibility.

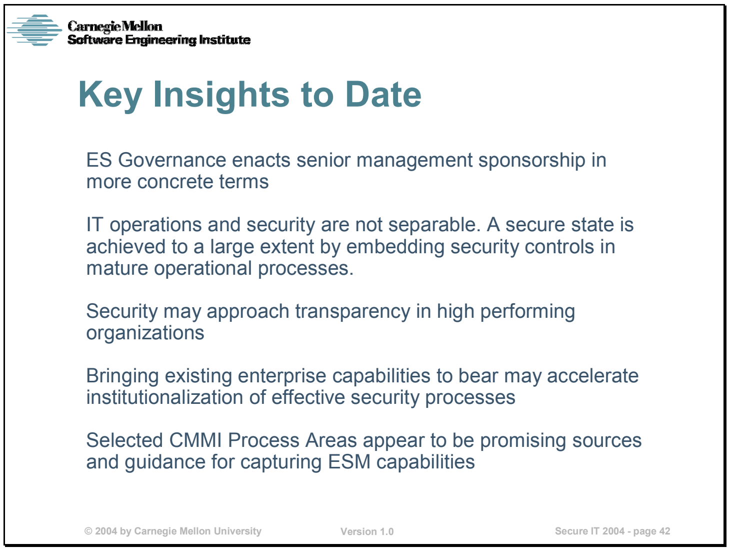
3. Rewards/reinforcements for personal heroics vs. repeatable, predictable discipline: There may be a cultural norm or a reward system (explicit or implicit) that encourages personal heroics. For instance, one person works throughout the night for an entire weekend fighting a fire and gets rewarded as the hero who saved the day. What is overlooked is that if one person can save the entire boat, one person can probably sink it too. In these organizations, implementing effective processes and controls may be resisted or actively rejected as too bureaucratic, almost as an immune system would resist an unknown and foreign object.

4. Continued argument that IT operations and security are different than other business investments or projects: Because of their technologically complex nature, IT and security are often not subjected to the same rigorous performance measures that demonstrate their value to the business as other business units. IT often operates as an insular stovepipe, often with a separate security stovepipe within it, to perpetuate this 'difference' claim, holding the organization hostage and at arm's length. When IT and security do not have defined roles where they are collectively solving common business objectives

with partnering business units, and where they are required to demonstrate business value, blame games and finger pointing for failures can ensue and drain precious resources and management attention.

5. A desire for a technical solution, which is easier to justify and implement than people and process improvements: Because of their background and experience, IT management values automation and technology (exciting) over repeatable processes and controls (boring and bureaucratic). In the absence of defined, implemented processes and controls, the deployment of new security technology solutions take precedence. This can result in the unintended consequence of automatically performing devastating, irreversible IT operational changes in mere seconds, resulting in potentially increasing amounts of unplanned work. Combined with the previous root causes, this factor perpetuates the continuing chaos.

Slide 42



Carnegie Mellon
Software Engineering Institute

Key Insights to Date

ES Governance enacts senior management sponsorship in more concrete terms

IT operations and security are not separable. A secure state is achieved to a large extent by embedding security controls in mature operational processes.

Security may approach transparency in high performing organizations

Bringing existing enterprise capabilities to bear may accelerate institutionalization of effective security processes

Selected CMMI Process Areas appear to be promising sources and guidance for capturing ESM capabilities

In summary, we have formulated the following insights and continue to examine and test them in the field and as we learn from high performing organizations:

A clear, concise description of the processes necessary to govern enterprise security makes explicit the actions and behaviors that senior managers must enact to bring about a culture of security, and in the process, be able to demonstrate due diligence and an acceptable standard of due care to their customers and communities.

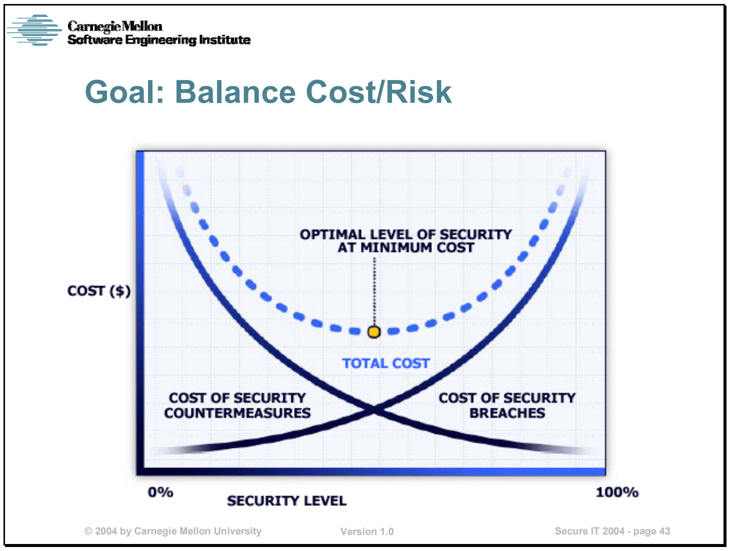
Effective security controls are embedded within mature IT operational processes. The two capabilities (security and IT operations) must work together to ensure this occurs, with appropriate project management and audit oversight.

High performing organizations that do security well do not think of it any differently than any other set of operational processes and controls.

Security lives in an organizational and operational context, not as a standalone discipline. This context has not been well defined from a security perspective. It includes all of an organization’s capabilities that need to be brought to bear to achieve and sustain a secure state. ESM takes what an organization is already doing well and applies these capabilities to managing security at an enterprise level, thus taking actions that are no different (conceptually) from those needed to meet any other requirement of conducting business. Examples of such capabilities include risk management, project management, and audit.

Extensive work has been done in the software development community to identify the basis for mature system/software engineering, development, and operations using a range of process areas documented in the SEI’s CMM and CMMI. We are drawing from this body of knowledge and experience to inform ESM capability area definitions.

Slide 43



Carnegie Mellon
Software Engineering Institute

Goal: Balance Cost/Risk

Version 1.0

This slide is complements of Bill Hancock, CISO, Cable and Wireless.

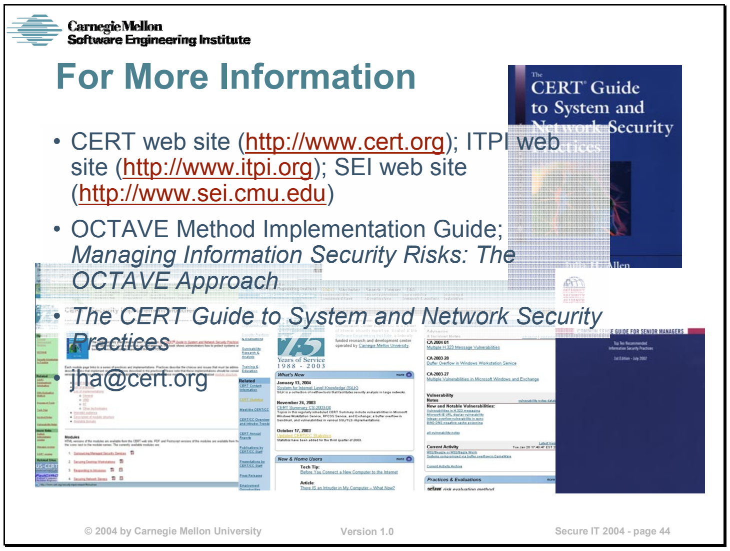
All organizations are attempting to define the right balance between cost and risk when it comes to making security investment decisions. Most organizations would benefit from a framework that allows them to determine their security posture with respect to their peers and define an acceptable level of security that is 'good enough.'

Consider the following perspectives when balancing cost and risk:

"Gartner estimates that the cost to mitigate damage from a successful attack is at least 50% higher than the cost to prevent it." Gartner. "Establish A Strong Defense in Cyberspace." CSO online, 2003. Available at http://www.csoonline.com/analyst/report1460.html

Gartner trends indicate that security is seen as a cost of doing business (2003), moving toward being treated as a legal exposure (2005), and evolving to a competitive advantage (2007), selling trust.

Slide 44



Carnegie Mellon
Software Engineering Institute

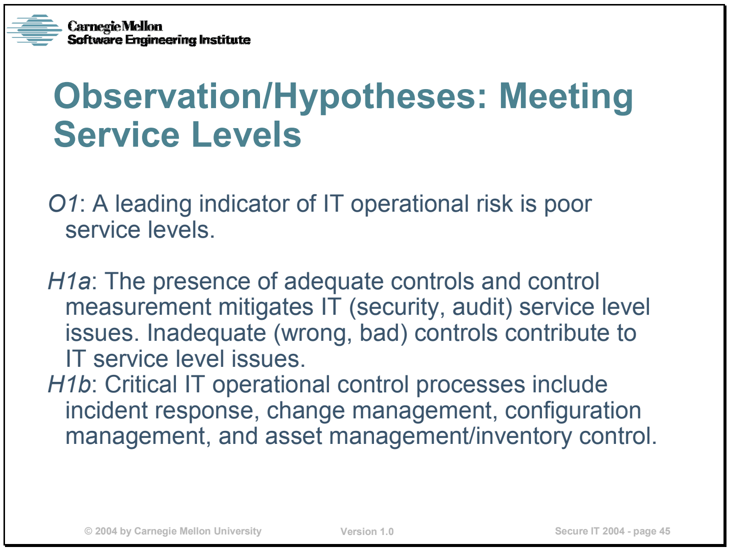
For More Information

- CERT web site (http://www.cert.org); ITPI web site (http://www.itpi.org); SEI web site (http://www.sei.cmu.edu)
- OCTAVE Method Implementation Guide; *Managing Information Security Risks: The OCTAVE Approach*
- *The CERT Guide to System and Network Security Practices*
- jha@cert.org

Caralli, Rich, et al. *The Critical Success Factors Method: Establishing a Foundation for Enterprise Security Management* (CMU/SEI-2004-TR-010). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, May 2004.

OCTAVE Method Implementation Guide: information available at http://www.cert.org/octave/omig.html.

The CERT Guide to System and Network Security Practices provides a detailed description of the practices necessary to harden and secure a general-purpose server (Chapter 2), a public web server (Chapter 3), and a firewall system (Chapter 4). It also has detailed descriptions of the practices required to Prepare, Detect, and Respond to an incident, and Improve following an incident. Information is available at http://www.awprofessional.com/title/020173723X.



Carnegie Mellon
Software Engineering Institute

Observation/Hypotheses: Meeting Service Levels

O1: A leading indicator of IT operational risk is poor service levels.

H1a: The presence of adequate controls and control measurement mitigates IT (security, audit) service level issues. Inadequate (wrong, bad) controls contribute to IT service level issues.

H1b: Critical IT operational control processes include incident response, change management, configuration management, and asset management/inventory control.

Capturing observations and forming hypotheses based on these derives from the scientific method and can serve as a useful structure for examining an issue and potential solutions. The Observations and Hypotheses presented here were drawn from interviews with Gene Kim and Kevin Behr based on their experiences with a wide range of customers. Julia Allen formulated these materials and presented them at the BIC SORT, to invite participants to challenge these statements and stimulate clarification and expansion. The content presented here represents a consensus of those attending.

To determine if a service level is poor, its baseline state needs to be defined, and it needs to be regularly measured and monitored. Poor service levels (those that do not meet business objectives as viewed by customers and users) are often manifest in the face of compromises of availability (most critical), confidentiality, and integrity.

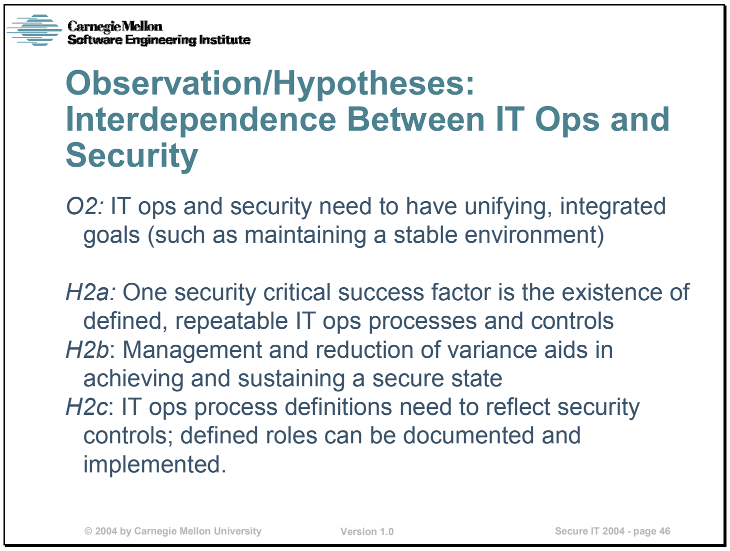
In addition to poor service levels, other leading indicators of IT operational risk include being subject to regulatory fines and the presence of unauthorized changes from any source (user, administrator, intruder).

Adequate controls and regularly measuring and monitoring these controls can mitigate against the occurrence or degree of service level issues. Service level issues can be caused by the absence of controls but just because controls are absent doesn't mean that an organization will necessarily have service level issues. Not all service level issues are caused by absence of controls. In other words, controls are necessary but sometimes not sufficient.

Additional solutions include overprovisioning (providing excess capacity) to anticipate service level issues that are not within the organization's control (such as peaks in demand).

Participants generally agreed that these hypotheses match their belief systems and the way their organizations work. Several have put a number of moderately rigid controls in place that people don't mind following because they are not too painful, and they prevent bad things from happening.

Slide 46



Carnegie Mellon
Software Engineering Institute

Observation/Hypotheses: Interdependence Between IT Ops and Security

O2: IT ops and security need to have unifying, integrated goals (such as maintaining a stable environment)

H2a: One security critical success factor is the existence of defined, repeatable IT ops processes and controls
H2b: Management and reduction of variance aids in achieving and sustaining a secure state
H2c: IT ops process definitions need to reflect security controls; defined roles can be documented and implemented.

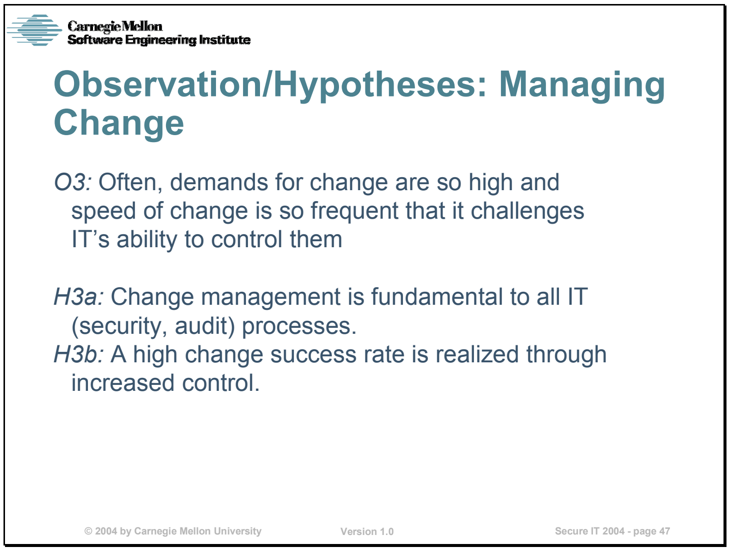
Several of the participants do not see IT operations and security as separate and, in fact, embed security controls in well defined IT operational processes. Security defines the controls and IT operations implements them. Security is responsible for monitoring the adequacy of the controls from a security perspective.

Some saw security as having competing or different goals from IT operations, while others did not. Both have the goal to maintain a stable environment that runs smoothly, even if they disagree on the approach. There is also interdependence between IT operations, security, and R&D (development, engineering). These three functions need to work in an integrated fashion across all three, not just pairwise.

Security needs to be centrally managed and then implemented in a decentralized fashion, in part within IT operations.

Managing and reducing variance in process performance (using methods such as Six Sigma) where security controls are part of ongoing IT operational processes does result in a higher level of security.

Slide 47



Carnegie Mellon
Software Engineering Institute

Observation/Hypotheses: Managing Change

O3: Often, demands for change are so high and speed of change is so frequent that it challenges IT's ability to control them

H3a: Change management is fundamental to all IT (security, audit) processes.
H3b: A high change success rate is realized through increased control.

© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 47

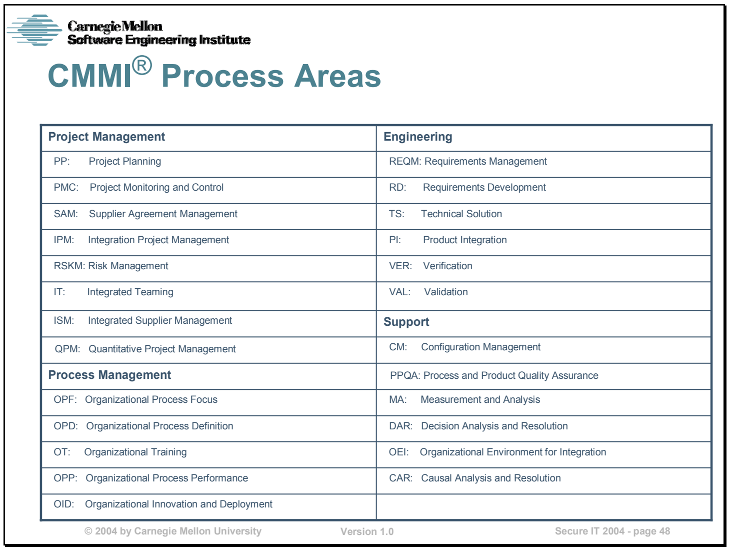
Changes come from many sources: software updates including security patches, new applications, technology changes, configuration changes, etc. Business demands for change are high and frequent and thus can cause disruptions, delays, or more serious impacts to service availability. In the absence of a change management process and appropriate controls, IT operations is often unable to respond effectively. In fact, many organizations do not believe control is possible.

A high change success rate is defined as the ratio of planned (authorized) to unplanned (unexpected, inadvertent) changes. The assertion is that if organizations mature processes and controls that address the part of the change management problem space that they can control, this will free up resources to focus more attention and energy on the part of the problem that is unpredictable.

Today IT operations and security functions are expected to prevent every bad thing from happening; if they can't prevent something from happening, they need to be able to detect it; if they can't detect it, they need to be able to recover from it and restore service in a timely manner. Effective change management aids in both prevention and detection. A contrasting view is to manage to a planned failure rate and allocate time and resources to take this into account.

Another way of stating hypothesis H3b is that change management does not slow things down, isn't bureaucratic, doesn't reduce productivity, and isn't burdensome. Change management properly done can enable, improve, and accelerate business/service level performance . In the absence of change management, there is often chaos. The only thing worse than having a change management process and supporting controls is not having these.

Slide 48



Carnegie Mellon
Software Engineering Institute

CMMI® Process Areas

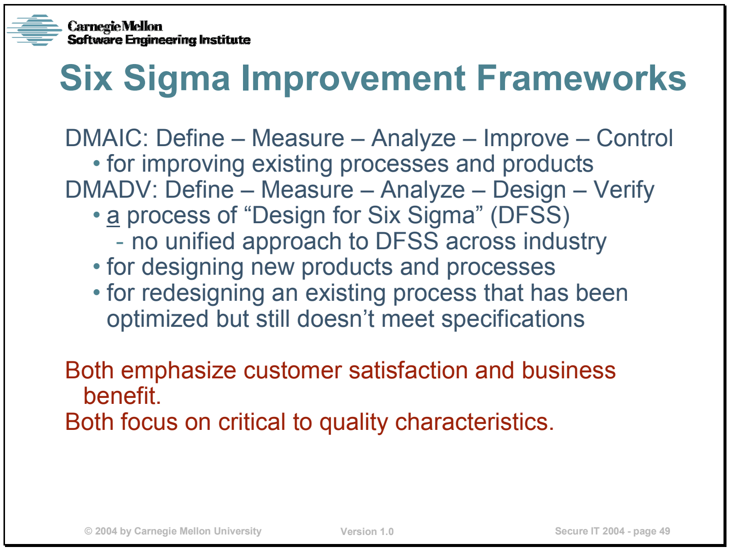
Project Management	Engineering
PP: Project Planning	REQM: Requirements Management
PMC: Project Monitoring and Control	RD: Requirements Development
SAM: Supplier Agreement Management	TS: Technical Solution
IPM: Integration Project Management	PI: Product Integration
RSKM: Risk Management	VER: Verification
IT: Integrated Teaming	VAL: Validation
ISM: Integrated Supplier Management	**Support**
QPM: Quantitative Project Management	CM: Configuration Management
Process Management	PPQA: Process and Product Quality Assurance
OPF: Organizational Process Focus	MA: Measurement and Analysis
OPD: Organizational Process Definition	DAR: Decision Analysis and Resolution
OT: Organizational Training	OEI: Organizational Environment for Integration
OPP: Organizational Process Performance	CAR: Causal Analysis and Resolution
OID: Organizational Innovation and Deployment	

Version 1.0 Secure IT 2004 - page 48

CMMI: Guidelines for Process Integration and Product Improvement; Mary Beth Chrissis, Mike Konrad, Sandy Shrum; Addison Wesley, 2003.

CMMI documents a community consensus of 25 process areas and 17 generic goals and practices required to develop and maintain products and services throughout the product life cycle (conception through delivery and maintenance). “A product can be an airplane, a digital camera, a video game component, an automated teller machine, a missile guidance system, or a software page available from a commercial retailer. It can also be a service such as delivering a training class, technical support for a software product, long-distance telephone services, data-processing services, and online banking.” The bodies of knowledge covered by CMMI include software engineering, systems engineering, integrated product and process development, supplier sourcing.

Slide 49



Six Sigma Improvement Frameworks

DMAIC: Define – Measure – Analyze – Improve – Control
- for improving existing processes and products

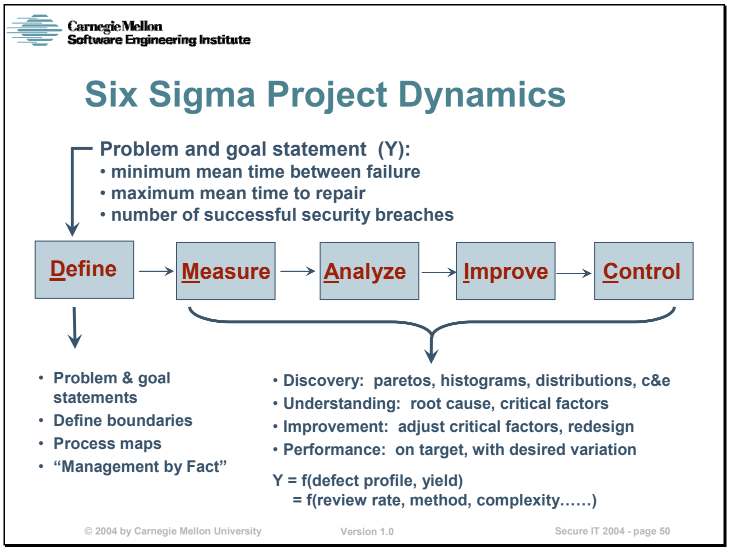
DMADV: Define – Measure – Analyze – Design – Verify
- a process of “Design for Six Sigma” (DFSS)
  - no unified approach to DFSS across industry
- for designing new products and processes
- for redesigning an existing process that has been optimized but still doesn’t meet specifications

Both emphasize customer satisfaction and business benefit.
Both focus on critical to quality characteristics.

There are a growing number of IT operations and security organizations who are either using or in the process of considering using Six Sigma methods, techniques, and tools to aid in achieving higher levels of customer satisfaction and service level performance. One definition of Six Sigma is “a statistical measure of the performance of a process or a product.” In Six Sigma, anything that is unacceptable to the customer in terms of a product or service is considered a *defect*. The DMAIC Framework appears to have the greatest applicability to IT operations and security based on its focus to improve existing processes.

D: make the links from the customer to the individual project or process; identify the ‘critical to quality’ factors as best as possible. CTQ factors are customer requirements and expectations.
M: gather supporting data, make sure it’s valid
A: decompose and analyze the data; look for control knobs
I: use knowledge of control knobs to identify improvements
C: use prevention/design and/or monitoring to ensure that performance does not degrade

Further information on Six Sigma can be found at http://www.isixsigma.com.



Carnegie Mellon
Software Engineering Institute

Six Sigma Project Dynamics

Problem and goal statement (Y):
- minimum mean time between failure
- maximum mean time to repair
- number of successful security breaches

Define → **Measure** → **Analyze** → **Improve** → **Control**

- Problem & goal statements
- Define boundaries
- Process maps
- "Management by Fact"

- Discovery: paretos, histograms, distributions, c&e
- Understanding: root cause, critical factors
- Improvement: adjust critical factors, redesign
- Performance: on target, with desired variation

Y = f(defect profile, yield)
= f(review rate, method, complexity……)

Version 1.0

In selecting a Six Sigma project, one needs to establish the importance to the business, typically in terms of cost savings of at least $100-150K (US), and a recommended duration of 3-6 months.

Six Sigma project objectives are quantitative and one or more of the following:

Improve customer satisfaction.

Optimize the supply chain.

Reduce defects.

Reduce cycle time.

Improve first-pass yield.

Reduce variability.

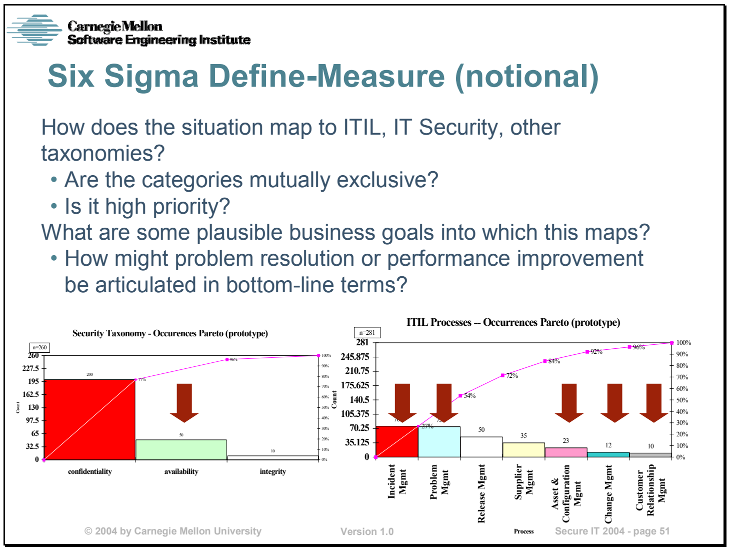
Optimize product performance.

Optimize process performance.

Reduce costs.

Reduce the cost of quality

This slide and the next one provide some notional descriptions of how Six Sigma could be applied to IT operations and security processes and controls.



Carnegie Mellon
Software Engineering Institute

Six Sigma Define-Measure (notional)

How does the situation map to ITIL, IT Security, other taxonomies?

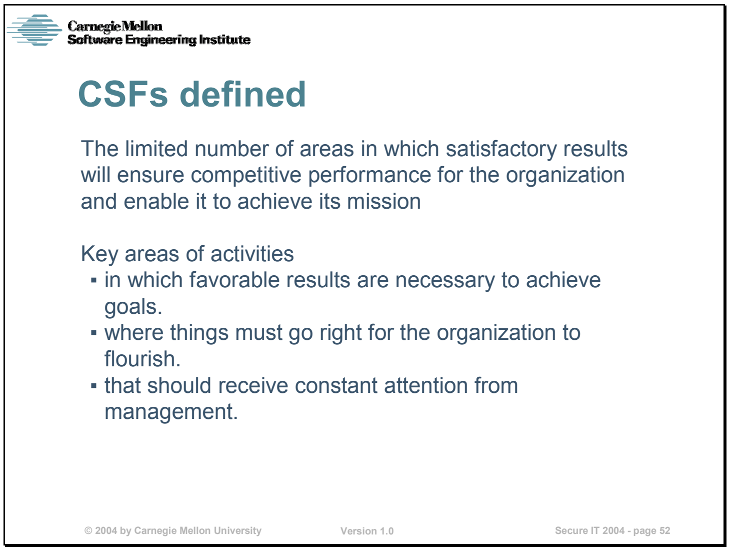
- Are the categories mutually exclusive?
- Is it high priority?

What are some plausible business goals into which this maps?

- How might problem resolution or performance improvement be articulated in bottom-line terms?

Security Taxonomy - Occurences Pareto (prototype)
n=260
260
227.5
195
162.5
130
97.5
65
32.5
0
Count
200
50
10
77%
96%
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Count
confidentiality
availability
integrity
ITIL Processes -- Occurrences Pareto (prototype)
n=281
281
245.875
210.75
175.625
140.5
105.375
70.25
35.125
0
50
35
23
12
10
27%
54%
72%
84%
92%
96%
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Incident Mgmt
Problem Mgmt
Release Mgmt
Supplier Mgmt
Asset & Configuration Mgmt
Change Mgmt
Customer Relationship Mgmt
Process

Slide 52



Carnegie Mellon
Software Engineering Institute

CSFs defined

The limited number of areas in which satisfactory results will ensure competitive performance for the organization and enable it to achieve its mission

Key areas of activities
- in which favorable results are necessary to achieve goals.
- where things must go right for the organization to flourish.
- that should receive constant attention from management.

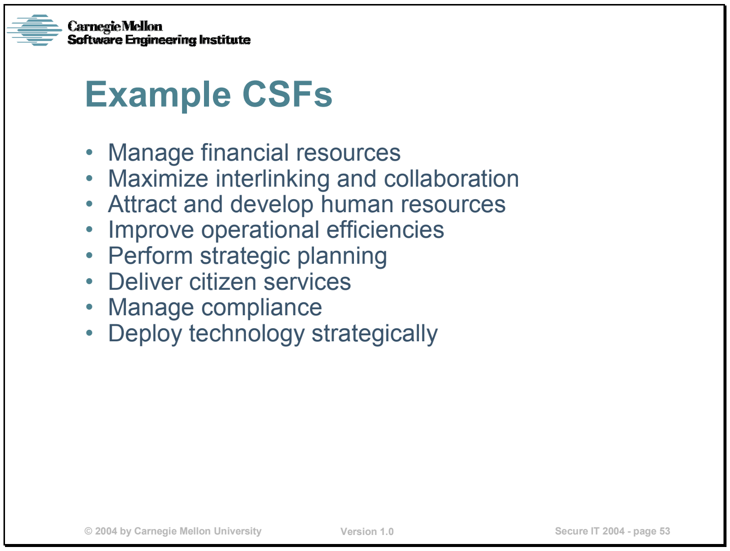
© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 52

As a part of MIT's Sloan School of Management, John F. Rockhart recognized the challenge that the onslaught of information presented to senior executives. In spite of the availability of more information, research showed that senior executives still lacked the information essential to make the kinds of decisions necessary to manage the enterprise. As a result, Rockhart's team concentrated on developing an approach to help executives clearly identify and define their information needs. Using success factors as a filter, management could identify the information that was most important to making critical enterprise decisions. Accordingly, decisions made in this manner should be more effective because they are based on data that is specifically linked to the organization's success factors.

In 1981, Rockhart codified a technique that embodied the principles of "success factors" as a way to systematically identify the information needs of executives. This work, presented in "A Primer on Critical Success Factors," detailed the steps necessary to collect and analyze data for the creation of a set of organizational CSFs [Rockhart 81]. This document is widely considered to be the earliest description of the CSF technique. An earlier description of this work is also presented in John F. Rockhart's article "Chief Executives Define Their Own Data Needs," Harvard Business Review, March-April, 1979.

The fact that critical success factors can be defined in so many different ways speaks to their elusive nature. Managers generally recognize their critical success factors when they see or hear them, but may be unable to clearly and concisely articulate them or appreciate their importance. In fact, most managers are aware of the variables they must manage to be successful, yet only when problems arise and root causes are identified are these variables made explicit. For example, suppose an organization finds an alarming number of duplicate payments to vendors. They might conclude that this problem is related to poor staff training or high levels of staff turnover. As a result, the effective management of human resources (attracting, training, retaining) might be identified as an important activity that can affect or impact the performance of their strategic goals. In the process, they have explicitly defined a critical success factor for the organization.

Critical success factors are powerful because they make explicit those things that a manager intuitively, repeatedly, and even perhaps accidentally knows and does to stay competitive. However, when made explicit, a critical success factor can tap the intuition of good managers and make it available to guide and direct the organization toward accomplishing its mission.



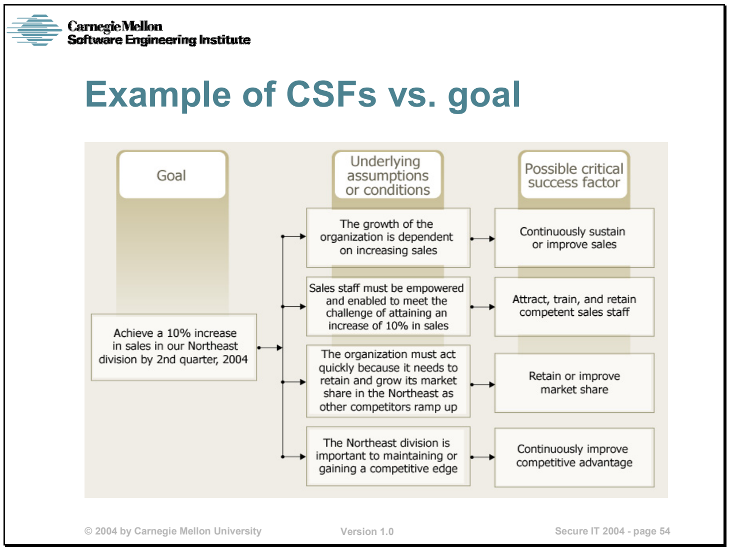
Carnegie Mellon
Software Engineering Institute

Example CSFs

- Manage financial resources
- Maximize interlinking and collaboration
- Attract and develop human resources
- Improve operational efficiencies
- Perform strategic planning
- Deliver citizen services
- Manage compliance
- Deploy technology strategically

These are examples of critical success factors that might be found in a wide range of organizations.

Slide 54



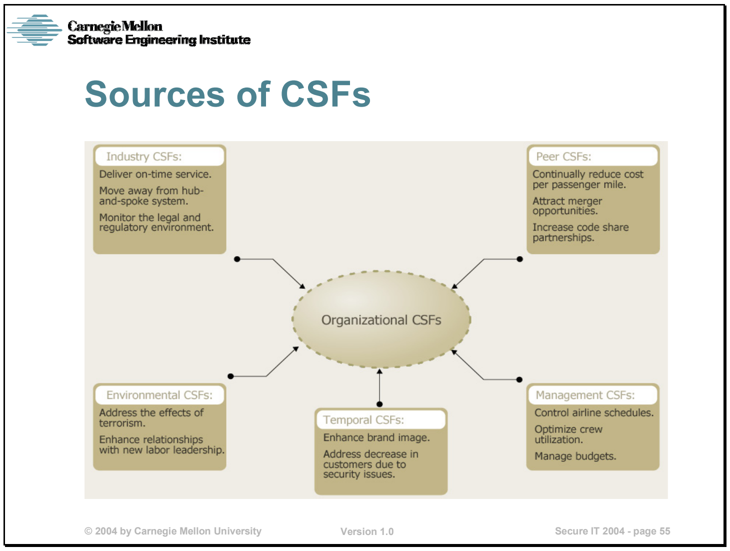
Carnegie Mellon
Software Engineering Institute

Example of CSFs vs. goal

Goal	Underlying assumptions or conditions	Possible critical success factor
Achieve a 10% increase in sales in our Northeast division by 2nd quarter, 2004	The growth of the organization is dependent on increasing sales	Continuously sustain or improve sales
	Sales staff must be empowered and enabled to meet the challenge of attaining an increase of 10% in sales	Attract, train, and retain competent sales staff
	The organization must act quickly because it needs to retain and grow its market share in the Northeast as other competitors ramp up	Retain or improve market share
	The Northeast division is important to maintaining or gaining a competitive edge	Continuously improve competitive advantage

It is unlikely that a one-to-one relationship exists between an organizational goal and a critical success factor. In reality, an organizational goal may be dependent on one or more critical success factor to be achieved. Conversely, a critical success factor may influence or affect the achievement of several different goals. The many-to-many relationship between goals and critical success factors is indicative of their interdependent nature and importance in helping the organization accomplish its mission.

Slide 55



Carnegie Mellon
Software Engineering Institute

Sources of CSFs

Industry CSFs:
Deliver on-time service.
Move away from hub-and-spoke system.
Monitor the legal and regulatory environment.

Peer CSFs:
Continually reduce cost per passenger mile.
Attract merger opportunities.
Increase code share partnerships.

Organizational CSFs

Environmental CSFs:
Address the effects of terrorism.
Enhance relationships with new labor leadership.

Temporal CSFs:
Enhance brand image.
Address decrease in customers due to security issues.

Management CSFs:
Control airline schedules.
Optimize crew utilization.
Manage budgets.

Critical success factors are generally described within the sphere of influence of a particular manager. But there are many levels of management in a typical organization, each of which may have slightly different operating environments. For example, executive-level managers may be focused on the external environment in which their organizations live, compete, and thrive. In contrast, line-level managers may be concerned with the operational details of the organization and therefore are focused on what they need to do to achieve their internal, operational goals. Because of these different operational domains, the critical success factors for the organization may come from many different sources. All are important for the organization as a whole to accomplish its mission, regardless of their source.

Rockhart defined five specific sources or types of critical success factorsfor the organization as follows:

the industry in which the organization competes or exists

an understanding of the organization’s peers

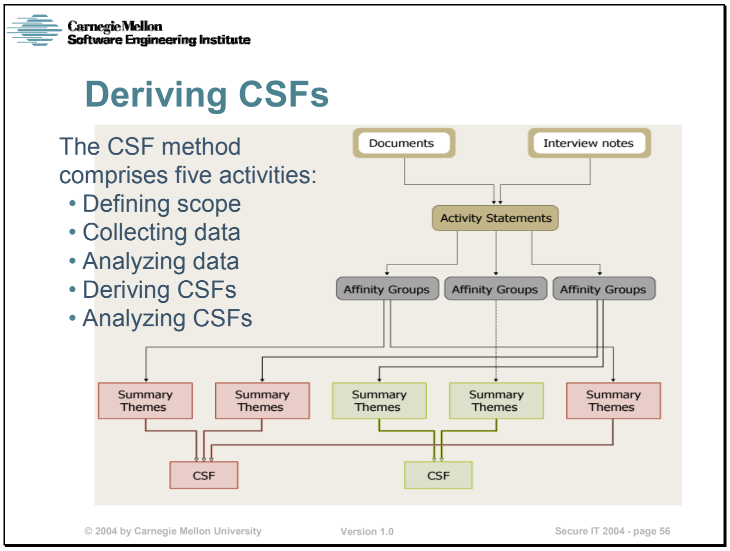
the general business climate or organizational environment

problems, barriers, or challenges to the organization

layers of management

To provide an accurate picture of an organization’s overall key performance areas, it is important to identify critical success factors from each of these sources. However, as we found in our use of the CSF method, deriving critical success factors at the highest levels of the organization tends to bring an acceptable mix of CSFs from many of these sources, so long as a broad cross section of management is represented in the process.

Slide 56


Documents
Interview notes
Activity Statements
Affinity Groups
Affinity Groups
Affinity Groups
Summary Themes
Summary Themes
Summary Themes
Summary Themes
Summary Themes
CSF
CSF

Carnegie Mellon
Software Engineering Institute

Deriving CSFs

The CSF method comprises five activities:

- Defining scope
- Collecting data
- Analyzing data
- Deriving CSFs
- Analyzing CSFs

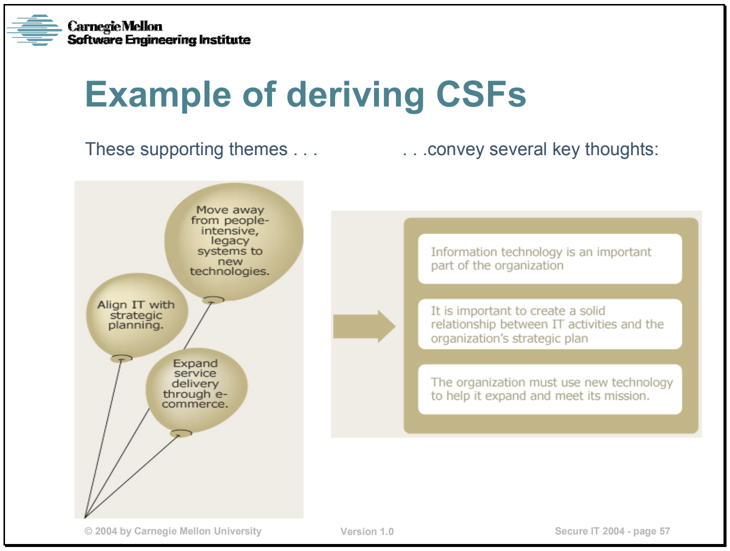
Version 1.0 Secure IT 2004 - page 56

Critical success factors are derived rather than created. They are extracted from raw data collected throughout the process and formed into activity statements, affinity groupings, and finally supporting themes. In our experience, we have found that critical success factors can be derived easily based on supporting themes alone if the process described herein is followed.

Critical success factors seem to have more clarity, usability, and impact when they can be reduced to a brief, concise statement that captures the CSF's essential intent and description. For example, one of the reasons that mission statements are often not able to be recited by employees is because they are generally too long and contain too much detail. A similar issue can be found with critical success factors—if it takes hundreds of words and paragraphs to define a CSF, there's a good chance that it isn't a key performance factor that the organization can reasonably achieve.

In our technique for creating CSFs, we have limited ourselves to as few words as possible (generally fewer than 10) when describing a critical success factor. For certain, a more detailed description of the meaning of the CSF, its origin, and potential impact on the organization can be developed, but won't be as useful or practical as a statement that can capture the CSF and can be easily recalled and communicated.

Slide 57



Carnegie Mellon
Software Engineering Institute

Example of deriving CSFs

These supporting themes . . .

Move away from people-intensive, legacy systems to new technologies.

Align IT with strategic planning.

Expand service delivery through e-commerce.

. . .convey several key thoughts:

- Information technology is an important part of the organization
- It is important to create a solid relationship between IT activities and the organization's strategic plan
- The organization must use new technology to help it expand and meet its mission.

© 2004 by Carnegie Mellon University Version 1.0 Secure IT 2004 - page 57

A simple process for deriving CSFs is to use supporting themes as a guide. The reason for developing supporting themes is to represent, in as few summary statements as possible, the things that managers are concerned about as reflected in activity statements. If the process of creating supporting themes is done correctly, the resulting themes should provide enough insight to "name" a critical success factor. For example, consider the following supporting themes:

Align information technology with strategic planning.

Expand service delivery through e-commerce.

Move away from people-intensive, legacy systems to newer technologies.

These supporting themes communicate several key notions. For example, information technology is an important part of the organization. Second, it is important to create a solid relationship between the information technology activities of the organization and the organization's strategic plan. Finally, the organization must use new technology to help it expand and meet its mission.